FortiClient - Administration Guide

Version 5.6.4

FORTINET DOCUMENT LIBRARY
http://docs.fortinet.com

FORTINET VIDEO GUIDE
http://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTIGATE COOKBOOK
http://cookbook.fortinet.com

FORTINET TRAINING SERVICES
http://www.fortinet.com/training

FORTIGUARD CENTER
http://www.fortiguard.com

END USER LICENSE AGREEMENT
http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdocs@fortinet.com

January 15, 2018
FortiClient 5.6.4 Administration Guide
04-564-400716-20180115

TABLE OF CONTENTS

Change Log

Date	Change Description
2018-01-08	Initial release of 5.6.4.
2018-01-15	Installing FortiClient using the CLI on page 39 added.

Introduction

FortiClient is an all-in-one comprehensive endpoint security solution that extends the power of Fortinet's Advanced Threat Protection (ATP) to end user devices. As the endpoint is the ultimate destination for malware that is seeking credentials, network access, and sensitive information, ensuring your endpoint security combines strong prevention with detection and mitigation is critical.

This document is written for FortiClient (Windows) 5.6.4. FortiClient 5.6.4 is not available for Mac OS X.

FortiClient modes and features

FortiClient is available in the following modes: Standalone mode and Managed mode.

Standalone mode

In standalone mode, FortiClient is not connected to FortiGate or EMS. In this mode, FortiClient is free for private individuals and commercial businesses to use; no license is required. See Getting started with standalone mode on page 19.

Support for FortiClient in standalone mode is provided on the Fortinet Forums (forum.fortinet.com). Phone support is not provided.

Managed mode

In managed mode, FortiClient is connected to EMS or FortiGate. Another option is to connect FortiClient to EMS and FortiGate. In managed mode, FortiClient licensing is applied to FortiGate or EMS. No separate license is required for FortiClient itself.

When connected only to EMS, FortiClient is managed by EMS. However, FortiClient cannot participate in network compliance or Fortinet Security Fabric.

When connected to FortiGate, FortiClient integrates with Security Fabric to provide endpoint awareness, compliance, and enforcement by sharing endpoint telemetry regardless of device location, such as corporate headquarters or a café. At its core, FortiClient automates prevention of known and unknown threats through its built-in host-based security stack and integration with FortiSandbox. FortiClient also provides secure remote access to corporate assets via VPN with native two-factor authentication coupled with single sign on.

FortiClient works cooperatively with Fortinet Security Fabric. This is done by extending it down to the endpoints to secure them via security profiles, by sharing endpoint telemetry to increase awareness of where systems, users, and data reside within an organization, and by enabling the implementation of proper segmentation to protect these endpoints.

At regular intervals, FortiClient sends telemetry data to the nearest associated FortiGate. This visibility coupled with built-in controls from FortiGate allows the security administrator to construct a policy to deny access to endpoints with known vulnerabilities or to quarantine compromised endpoints with a single click.

See Getting started with managed mode on page 20.

Feature comparison of standalone and managed modes

The following table provides a feature comparison between standalone FortiClient (free version) and managed FortiClient (licensed version).

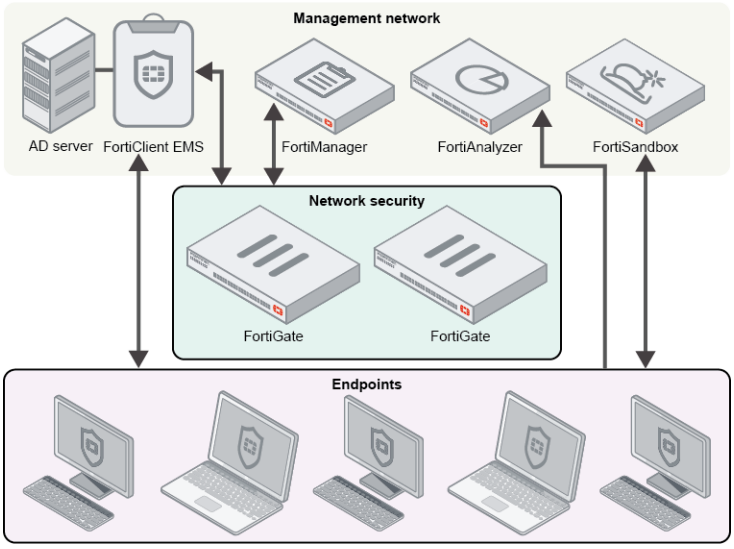
Both modes (free and licensed)	Only with managed mode (licensed)
Installation options • Security Fabric Agent: Telemetry, vulnerability scanning, vulnerability patching • Secure Remote Access: SSL and IPsec VPN components • Advanced Persistent Threat (APT): FortiSandbox detection and quarantine components • Additional Security Features: AntiVirus, Web Filtering, Single Sign On, Application Firewall. Select one, two, or all of the additional security features.	**Security Fabric and network access compliance** • Participation in Security Fabric • Compliance status • Define and enforce enterprise security policies when FortiClient used with FortiGate
Advanced Persistent Threat • Integration with FortiSandbox	**Central monitoring and management** • Centralized FortiClient monitoring with FortiGate or EMS • Centralized configuration provisioning and deployment when FortiClient used with EMS
AntiVirus • Realtime Antivirus protection • Antirootkit/antimalware • Grayware blocking (adware/riskware)	**Central logging** • Upload logs to FortiAnalyzer or FortiManager. FortiClient must connect to FortiGate or EMS to upload logs to FortiAnalyzer or FortiManager.
Web security • Web filtering • YouTube education filter	
Application control • Application Firewall • Block specific application traffic	

Both modes (free and licensed)	Only with managed mode (licensed)
Remote access • SSL VPN • IPsec VPN • Client certificate support • X.509 certificate support • Elliptical Curve certificate support • Two-factor authentication	
Vulnerability management • Vulnerability scanning • Links to FortiGuard with information on the impact and recommended actions • Automatic software patching for identifies vulnerabilities • List of software that requires manual installation of software patches	
Logging • VPN, Application Firewall, Antivirus, Web Filter, Update, and Vulnerability Scan logging • View logs locally	

Fortinet product support for FortiClient

The following Fortinet products work together to support FortiClient in managed mode:

- FortiClient EMS
- FortiManager
- FortiGate
- FortiAnalyzer
- FortiSandbox



FortiClient EMS

FortiClient EMS runs on a Windows server. EMS can manage FortiClient endpoints by deploying FortiClient (Windows) and profiles to endpoints, and the endpoints can connect FortiClient Telemetry to FortiGate or EMS. FortiClient endpoints connect to FortiGate to participate in Security Fabric or compliance enforcement. FortiClient endpoints connect to EMS to be managed in real time.

For information on EMS, see the *FortiClient EMS Administration Guide*, available in the Fortinet Document Library.

FortiManager

FortiManager provides central FortiClient management for FortiGate devices managed by FortiManager. In FortiManager, you can create one or more FortiClient profiles to assign to multiple FortiGate devices. You can also import FortiClient profiles from one FortiGate device and assign the FortiClient profile to other FortiGate devices. When endpoints are connected to managed FortiGate devices, you can use FortiManager to monitor endpoints from multiple FortiGate devices.

For information on FortiManager, see the *FortiManager Administration Guide*, available in the Fortinet Document Library.

FortiGate

FortiGate provides network security. FortiGate devices define compliance rules for NAC (network access control) for connected endpoints, and FortiClient communicates the compliance rules from FortiGate to endpoints. When FortiManager is used, FortiGate devices communicate between endpoints, EMS, and FortiManager.

When FortiClient Telemetry is connected to FortiGate, endpoints can participate in Security Fabric or compliance enforcement.

For information on FortiGate, see the *FortiOS Handbook*, available in the Fortinet Document Library.

FortiAnalyzer

FortiAnalyzer can receive logs from endpoints connected to FortiGate or EMS, and you can use FortiAnalyzer to analyze the logs and run reports. FortiAnalyzer receives logs directly from FortiClient.

For information on FortiAnalyzer, see the *FortiAnalyzer Administration Guide*, available in the Fortinet Document Library.

FortiSandbox

FortiSandbox offers the capabilities to analyze new, previously unknown, and undetected virus samples in real time. Files sent to it are scanned first, using similar Antivirus (AV) engine and signatures as are available on FortiOS and FortiClient. If the file is not detected but is an executable file, it is run in a Microsoft Windows virtual machine (VM) and monitored. The file is given a rating or score based on its activities and behavior in the VM.

As FortiSandbox receives files for scanning from various sources, it collects and generates AV signatures for such samples. FortiClient periodically downloads the latest AV signatures from the FortiSandbox, and applies them locally to all realtime and on-demand AV scanning.

For more information, see the *FortiSandbox Administration Guide*, available in the Fortinet Document Library.

This feature requires a FortiSandbox running version 2.1 or newer and is only available on FortiClient (Windows).

What's New in FortiClient 5.6

The following is a list of new features and enhancements in FortiClient 5.6.

FortiClient 5.6.4

There are no new features in FortiClient version 5.6.4.

FortiClient 5.6.4 is only available for FortiClient (Windows); FortiClient 5.6.4 is not available for FortiClient (Mac OS X).

FortiClient 5.6.3

There are no new features in FortiClient version 5.6.3.

FortiClient 5.6.2

There are no new features in FortiClient version 5.6.2.

FortiClient 5.6.2 is only available for FortiClient (Windows); FortiClient 5.6.2 is not available for FortiClient (Mac OS X).

FortiClient 5.6.1

The following is a list of new features in FortiClient version 5.6.1.

FortiClient 5.6.1 is only available for FortiClient (Mac OS X); FortiClient 5.6.1 is not available for FortiClient (Windows). The features below are available for FortiClient (Windows) 5.6.2 and higher.

Anti-exploit detection

The anti-exploit detection feature helps protect vulnerable endpoints from unknown exploit attacks. FortiClient monitors the behavior of popular applications, such as web browsers (Internet Explorer, Chrome, Firefox, Opera), Java/Flash plug-ins, Microsoft Office applications, and PDF readers, against exploits that use zero-day or unpatched vulnerabilities to infect the endpoint. Once detected, the compromised application process is terminated. The anti-exploit detection feature also helps protect against memory-based attacks and drive-by download attacks. It also detects and blocks unknown and known exploit kits. It is a signature-less solution. See Protecting applications from exploits on page 93.

The anti-exploit detection feature is currently available only for FortiClient (Windows).

Endpoint user's social IDs shared with FortiAnalyzer

When FortiClient is in managed mode, details from cloud applications about the endpoint user are sent to FortiAnalyzer. Before the information can be sent, the endpoint user must add the information to FortiClient by logging into a cloud application. See Retrieving user details from cloud applications on page 55.

Support for FortiSandbox authorization

Administrators can now enforce that only authorized FortiClient endpoints can connect to their FortiSandbox because the method for authorizing FortiClient has been improved. This feature requires FortiSandbox 2.5.0 or later.

You can now also use FortiClient Console to check whether FortiClient has been authorized for FortiSandbox scanning. See Checking FortiClient authorization for FortiSandbox scanning on page 69.

Improvements to VPN auto-connect

Various improvements and bug fixes have been made to improve the reliability and function of the VPN auto-connect feature. For example, if a VPN connection fails, a popup displays to inform the endpoint user about the connection failure while FortiClient continues trying to reconnect VPN in the background. Depending on the VPN configuration, the popup may include a *Cancel* button. If you click the *Cancel* button, FortiClient stops trying to reconnect VPN.

Contact information for endpoint users

Endpoint users can now manually add contact information such as email address and phone number to FortiClient Console. See Adding phone number and email address manually on page 57.

FortiClient 5.6.0

The following is a list of new features in FortiClient version 5.6.0.

FortiClient install option

FortiClient installers now only install features required for the solution chosen by the user at the time of install. See FortiClient setup types and modules on page 30.

Improved FortiClient compliance feature

FortiClient endpoint compliance is now enforced by FortiOS, where the administrator can warn or block non-compliant endpoints. The FortiClient dashboard displays the compliance status and reason for non-compliance. The FortiClient dashboard also includes information on the configuration settings causing non-compliance. See Compliance on page 49.

Vulnerability Scan supports FortiClient (Mac OS X)

The Vulnerability Scan and auto-patching feature is now supported in FortiClient (Mac OS X).

Vulnerability Scan GUI

The FortiClient GUI for the Vulnerability feature has been improved to show details on detected vulnerabilities and patch status and to identify software failed to be auto-patched. The improved display of the results helps improve usability, where the user can easily identify outstanding vulnerabilities that may need to be fixed manually. See Vulnerability Scan on page 123.

User avatar retrieval from cloud applications

FortiClient can now be used to retrieve usernames and user avatars from third-party cloud applications, such as LinkedIn, Salesforce, and Google. See Specifying user picture manually on page 57.

User avatar sent to FortiAnalyzer

FortiClient can now send user avatars and device information to FortiAnalyzer so it can be used in FortiView and reports.

Improved remote logging to FortiAnalyzer

FortiClient endpoints now send detailed logs to FortiAnalyzer so that data can be used for FortiView and custom reports. See Logging on page 130.

Sandbox detection for FortiClient (Windows)

With FortiClient (Windows), the Sandbox Detection feature can be used to send files to FortiSandbox for analysis without having to install the AntiVirus feature. This feature can use used with other third-party AV products installed on the endpoint. See Sandbox Detection on page 68.

New SSL VPN Windows driver for FortiClient (Windows)

A new SSL VPN Windows driver has been introduced with FortiClient (Windows), which will help resolve various SSL VPN connection issues. The new driver will help increase the performance by 20% and provide a stable VPN connection.

VPN auto-reconnect improvement

When the FortiClient VPN auto-connect feature is turned on, and VPN connection fails, a permanent popup displays to inform the user about the connection failure. FortiClient keeps retrying to connect VPN in the background until the user selects an option from the popup.

Configurator and Rebranding Tools

FortiClient Configurator Tool, which is used to create custom installers, is available for download for free from Fortinet Developer Network site (http://fndn.fortinet.net/). FortiClient Rebranding Tool is available for download with FNDN site license.

FortiClient Rebranding Tool is currently only available for FortiClient (Windows).

Getting Started

FortiClient can be used in standalone or managed mode. This section describes how to get started with each mode. It also includes the key concepts that administrators and endpoint users should be aware of when using FortiClient in managed mode.

Getting started with standalone mode

In standalone mode, FortiClient software is installed to computers or devices that have Internet access and are running a supported operating system. After FortiClient is installed, FortiClient automatically connects to FortiGuard Center (http://www.fortiguard.com) to protect the computer or device.

To get started with FortiClient in standalone mode:

1. Prepare to install FortiClient. See Provisioning Preparation on page 28.
   During installation, endpoint users choose which FortiClient modules to install. See FortiClient setup types and modules on page 30.
2. Install FortiClient on computers or devices with Internet access. See Provisioning on page 34.
3. Launch FortiClient Console.
   FortiClient connects to the Fortinet FortiGuard server to protect the computer.
4. Configure FortiClient settings. See Settings on page 130.
5. Configure the installed components.
   Depending on what FortiClient modules were installed, endpoint users can configure one, more, or all of the following modules:
   - Sandbox Detection—see Sandbox Detection on page 68.
   - Antivirus—see Antivirus on page 81.
   - Web Security—see Web Security/Web Filter on page 97.
   - Remote access—see Remote Access on page 108.
6. Use the installed modules using the tabs in FortiClient Console.
   Depending on what modules were installed, one, more, or all of the following tabs are available in FortiClient Console:
   - Sandbox Detection
   - Antivirus
   - Web Security
   - Remote Access
   - Vulnerability Scan—see Vulnerability Scan on page 123.

The *Compliance* tab is visible but not used in standalone mode.

Getting started with managed mode

In managed mode, FortiClient software is used with FortiGate or EMS. Another option is integrated mode where FortiGate and EMS are used together with FortiClient.

In managed mode, FortiClient software is installed to computers or devices on your network that have Internet access and are running a supported operating system. The computers or devices are referred to as endpoints. After FortiClient software is installed on endpoints, FortiClient performs the following actions:

- Automatically connects to FortiGuard Center (http://www.fortiguard.com) to protect the endpoint
- Automatically attempts to connect FortiClient Telemetry to FortiGate or EMS

The endpoint user confirms the request to complete the FortiClient Telemetry connection to FortiGate or EMS.

Administrators can optionally configure a FortiClient Telemetry connection that requires no confirmation by the endpoint user. See Custom FortiClient installation files and rebranding on page 32.

After FortiClient Telemetry is connected to FortiGate or EMS, FortiClient receives a profile from FortiGate and/or EMS, and the endpoint is managed.

To get started with FortiClient in managed mode:

1. (Administrators) Configure FortiGate and/or EMS to work with FortiClient.
   The following table identifies where to find information about configuring FortiGate and EMS.

FortiGate	See the *FortiOS Handbook - Security Profiles*.
EMS	See the *FortiClient EMS Administration Guide*.

2. (Administrators) Prepare to provision FortiClient. See Provisioning Preparation on page 28.
   Administrators can choose which FortiClient modules to install. See FortiClient setup types and modules on page 30.
3. (Administrators) Provision FortiClient on endpoints. See Provisioning on page 34.
   After FortiClient installs on endpoints, FortiClient Telemetry attempts connection to FortiGate or EMS. See FortiClient Telemetry on page 45.
   After FortiClient Telemetry connects to FortiGate or EMS, FortiClient receives a profile from FortiGate and/or EMS. The computer with FortiClient installed and FortiClient Telemetry connected is now a managed endpoint.
4. (Administrators) Manage endpoints using EMS. Administrators can also use FortiOS to monitor endpoints.
5. (Endpoint users) Configure the installed components using FortiClient Console.
   Depending on what FortiClient modules were installed, whether FortiGate compliance rules are used, and whether an EMS administrator has locked settings, endpoint users can configure none or some of the following modules:
   - Sandbox Detection
   - AntiVirus
   - Web Filter
   - Application Firewall
   - Remote Access

6. (Endpoint users) Use the installed modules in FortiClient Console.
   Depending on what modules were installed, one, more, or all of the following tabs are available in FortiClient Console:
   - Compliance
   - Sandbox Detection
   - AntiVirus
   - Web Filter
   - Application Firewall
   - Remote Access
   - Vulnerability Scan

Managed mode concepts

This section introduces the following concepts related to administering FortiClient in managed mode:

In FortiOS, administrators configure a *FortiClient Profile*, and in EMS administrators configure an *endpoint profile*, and these profiles can be downloaded to FortiClient in managed mode. Unless referring specifically to a profile created by using FortiOS or EMS, this guide uses the term *profile* when referring to a FortiClient Profile or endpoint profile received by FortiClient.

Terminology

The following clarifies the terminology used in the following sections.

Term	Definition
Managed mode	FortiClient used with FortiGate or EMS.
Integrated mode	FortiClient used with FortiGate and EMS. In this scenario, FortiClient connects FortiClient Telemetry to FortiOS and EMS.
Primary Telemetry connection	The following are primary Telemetry connections: • Connection between FortiClient and FortiOS when FortiClient is used with FortiGate. • Connection between FortiClient and EMS when FortiClient is used without FortiGate and the user manually connects FortiClient Telemetry to EMS.

Term	Definition
Secondary Telemetry connection	The following are secondary Telemetry connections: • Connection between FortiClient and EMS when FortiClient is used with FortiGate and EMS. • Connection between FortiClient and EMS when FortiClient is used without FortiGate and FortiClient is deployed using an installer created in EMS or gateway IP lists are used to connect FortiClient and EMS.
Connect FortiClient Telemetry	Establish connection between FortiClient and FortiGate or FortiClient and EMS. This is also referred to as registering FortiClient to FortiGate/EMS.
Profile	XML configuration file provided from FortiGate or EMS to the endpoint when in managed or integrated mode. In FortiOS, administrators configure a *FortiClient Profile*. This profile defines compliance rules for endpoint access to the network through FortiGate. It also defines how FortiGate handles endpoints that fail to comply with compliance rules. In EMS, administrators configure an *endpoint profile*. This profile defines the configuration for FortiClient software on endpoints. Unless referring specifically to a profile created using FortiOS or EMS, this guide uses the term profile when referring to a FortiClient Profile or an endpoint profile received by FortiClient.

FortiGate and FortiClient profiles

In FortiOS, administrators can configure a FortiClient profile and apply the profile to endpoints. The profile achieves the following goals:

- Defines compliance rules for endpoint access to the network through FortiGate
- Defines the non-compliance action for FortiGate—that is, how FortiGate handles endpoints that fail to comply with compliance rules

Compliance rules

FortiGate compliance rules define what configuration FortiClient software and the endpoint must have for the endpoint to maintain access to the network through FortiGate. The following is a sample of the compliance rules that administrators can enable or disable in a FortiClient profile using the FortiOS GUI:

- Telemetry data
- Endpoint Vulnerability Scan on client
- System compliance:
  - Minimum FortiClient version
  - What log types FortiClient will send to FortiAnalyzer
- Security posture check:
  - Realtime protection
  - Third party Antivirus on Windows

- Web filter
- Application firewall

Administrators can also define additional compliance rules using the FortiOS CLI.

Although the compliance rules define what configuration FortiClient software and the endpoint must have, the FortiClient profile from FortiGate does not include any configuration information. The endpoint user or administrator is responsible for configuring FortiClient Console to adhere to the compliance rules. An administrator can use EMS to configure FortiClient Console.

Non-compliance action

In addition to compliance rules, the FortiClient profile also defines how FortiGate will handle endpoints with a non-compliant status. FortiGate can block and quarantine endpoints, or FortiGate can warn endpoints about the non-compliant status, but allow network access. Administrators set the rules and non-compliance action using FortiOS, and FortiGate enforces the rules.

FortiGate 5.6.0 enforces compliance rules for FortiClient endpoints.

FortiClient Console displays compliant and non-compliant status and information about how endpoint users can return non-compliant endpoints to a status of compliance. The administrator or endpoint user is responsible for reading the information in FortiClient Console and updating FortiClient software on the endpoint to adhere to the compliance rules. Endpoint users can edit settings in FortiClient Console that are not controlled by the compliance rules or EMS.

Compliance rules configured using the CLI

When using FortiOS to create FortiClient profiles, administrators can configure some rules only by using the FortiOS CLI. Administrators must use the CLI to configure the following options:

- Allowed operating system for endpoints
- Registry entries for endpoints
- File in the file system on endpoints

See the *FortiOS CLI Reference*.

EMS and endpoint profiles

In EMS, administrators can configure an endpoint profile and apply the profile to endpoints. The profile defines the configuration for FortiClient software on endpoints. Administrators can also use the endpoint profile to install and upgrade FortiClient on endpoints. The profile consists of the following sections:

- Deployment
- AntiVirus
- Sandbox
- Web Filter

- Firewall
- VPN
- Vulnerability Scan
- System Settings
- XML Configuration

When the endpoint receives the configuration information in the endpoint profile, the settings in FortiClient Console are automatically updated. Settings in FortiClient Console are locked and read-only when EMS provides the configuration in a profile.

For information on configuring endpoint profiles using EMS, see the *FortiClient EMS Administration Guide*, available in the Fortinet Document Library.

Telemetry connection options

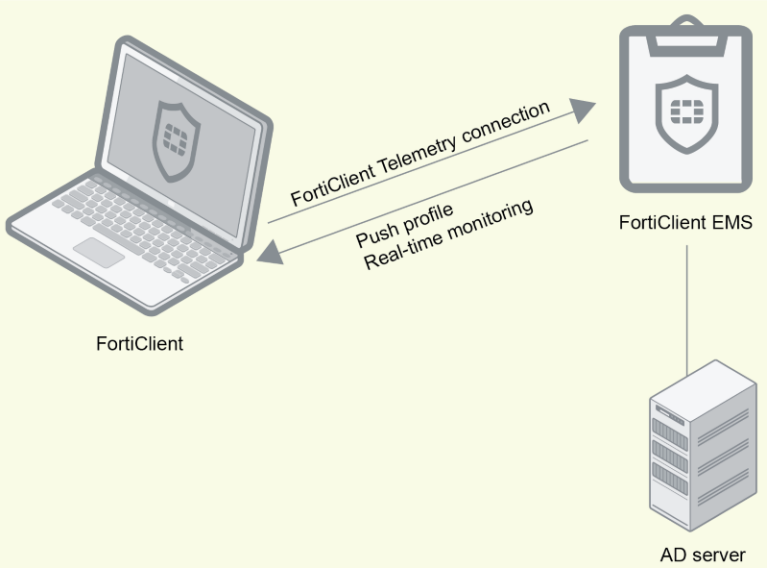
FortiClient Telemetry can connect to the following products:

- EMS—see EMS on page 24.
- FortiGate—see FortiGate on page 25.
- FortiGate and EMS in integrated mode—see FortiGate and EMS integration on page 25.

EMS manages FortiClient endpoints using the FortiClient Telemetry connection. Endpoints connect FortiClient Telemetry to FortiGate to participate in Security Fabric or compliance enforcement. FortiGate units do not manage endpoints.

EMS

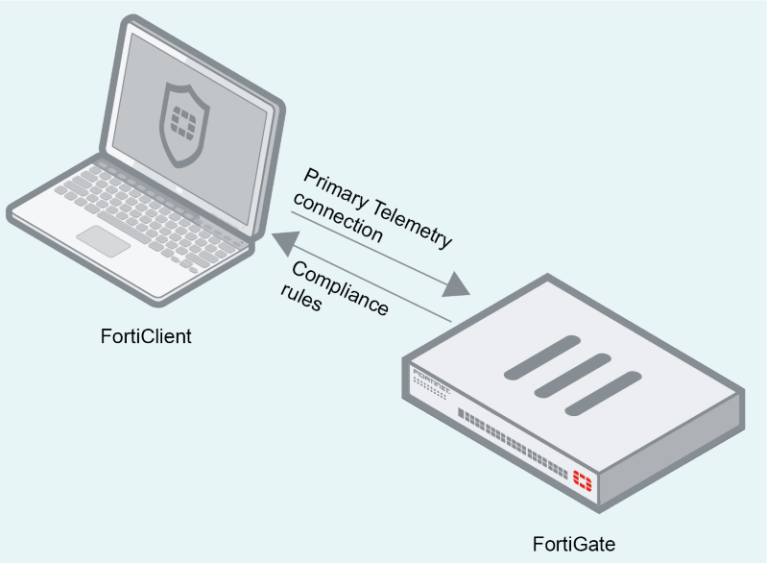
In this configuration, FortiClient Telemetry connects to EMS, and FortiClient receives a profile from EMS. The profile contains the configuration information for FortiClient, and EMS manages FortiClient endpoints. Network Access Control (NAC) and compliance are not supported.



Depending on how FortiClient was connected to EMS, this connection can be a primary or secondary Telemetry connection. See the *FortiClient Compliance Guide*, available at https://docs.fortinet.com/forticlient/admin-guides.

FortiGate

In this configuration, FortiClient Telemetry is connected to FortiGate, and FortiClient receives a profile from FortiGate. The profile contains the compliance rules for FortiClient, but not any configuration information for FortiClient. NAC and compliance can be supported.



FortiGate and EMS integration

In this configuration, FortiClient Telemetry connects to FortiGate to receive compliance rules. This is the primary Telemetry connection. NAC and compliance are supported. FortiClient Telemetry also connects to EMS to receive a profile of configuration information. This is the secondary Telemetry connection. This configuration is sometimes called integrated mode.

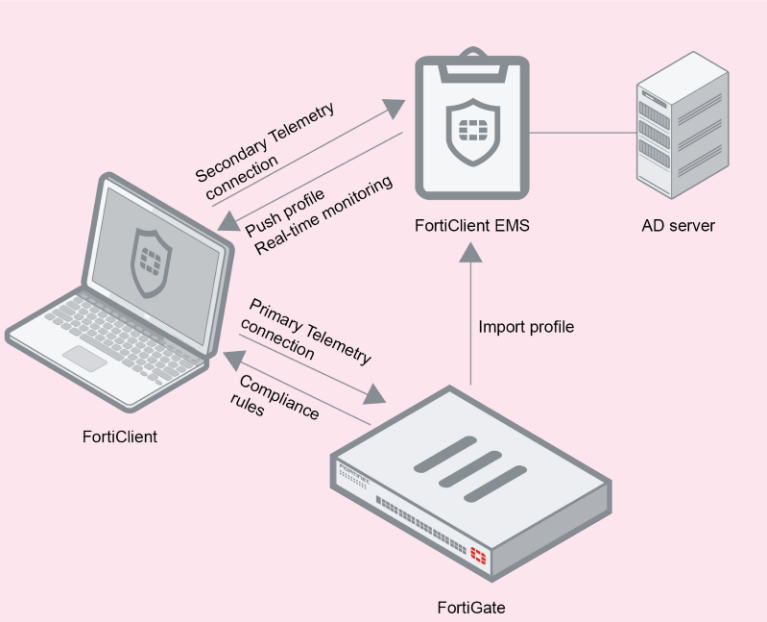
FortiGate does not provide configuration information for FortiClient and the endpoint. Endpoint users must manually configure FortiClient Console or an administrator must configure FortiClient using an EMS endpoint profile.

Following is a summary of how the FortiClient Telemetry connection works in integrated mode:

- FortiClient Telemetry connects to FortiGate. This is the primary FortiClient Telemetry connection.
- FortiClient Telemetry connects to EMS. This is the secondary FortiClient Telemetry connection.
- FortiClient receives a profile of compliance rules from FortiGate.
- FortiClient receives a profile of configuration information from EMS.

Administrators should ensure the configuration information from EMS matches the compliance rules set on FortiGate to avoid conflicting settings.

EMS can also import a profile from FortiOS, then push it to FortiClient.



Telemetry gateway IP lists

The Telemetry gateway IP list is a list of gateway IP addresses that FortiClient in managed mode can use to connect FortiClient Telemetry to FortiGate or EMS. After FortiClient installation completes on the endpoint, FortiClient automatically launches and uses the Telemetry gateway IP list to locate FortiGate and/or EMS for FortiClient Telemetry connection.

After FortiClient is installed on the endpoint and FortiClient Telemetry is connected to FortiGate and/or EMS, endpoint users can view the Telemetry gateway IP list in FortiClient Console. See Viewing gateway IP lists on page 58.

Configure Telemetry gateway IP lists (EMS)

FortiClient EMS includes the option to create one or more Telemetry gateway IP lists. The list can include IP addresses for EMS and for FortiGate. Administrators can assign Telemetry gateway IP lists to domains and workgroups in EMS. Administrators can also update the assigned Telemetry gateway IP lists after FortiClient is installed, and the updated lists are pushed to endpoints. See the *FortiClient EMS Administration Guide*.

Configure Telemetry gateway IP lists (FortiGate)

If administrators are using FortiGate without EMS, administrators can add Telemetry gateway IP addresses to the FortiClient installer using the Configurator Tool. See Custom FortiClient installation files and rebranding on page 32.

EMS and automatic upgrade of FortiClient

When EMS is used to manage FortiClient endpoints, you can use EMS to create a FortiClient installer that is configured to automatically upgrade FortiClient on endpoints to the latest version.

After the FortiClient installer with automatic upgrade enabled is deployed to endpoints, FortiClient is automatically upgraded to the latest version when a new version of FortiClient is available via EMS. See the *FortiClient EMS Administration Guide*.

Provisioning Preparation

Before provisioning FortiClient, administrators and endpoint users should understand the installation requirements and the FortiClient setup types available for installation. Administrators should also be aware of the licensing requirements if you are installing FortiClient in managed mode.

This section also identifies what firmware images and tools are available for FortiClient and where you can download the FortiClient installers.

Installation requirements

The following table lists operating system support and the minimum system requirements.

Operating system support	Minimum system requirements
• Microsoft Windows 7 (32-bit and 64-bit) • Microsoft Windows 8 (32-bit and 64-bit) • Microsoft Windows 8.1 (32-bit and 64-bit) • Microsoft Windows 10 (32-bit and 64-bit) FortiClient 5.6.4 does not support Microsoft Windows XP and Microsoft Windows Vista.	• Microsoft Internet Explorer version 8 or later • Microsoft Windows compatible computer with Intel processor or equivalent • Compatible operating system and minimum 512 MB RAM • 600 MB free hard disk space • Native Microsoft TCP/IP communication protocol • Native Microsoft PPP dialer for dial-up connections • Ethernet NIC for network connections • Wireless adapter for wireless network connections • Adobe Acrobat Reader for documentation • MSI installer 3.0 or later.
• Microsoft Windows Server 2008 R2 or newer	• Microsoft Internet Explorer version 8 or later • Microsoft Windows compatible computer with Intel processor or equivalent • Compatible operating system and minimum 512 MB RAM • 600 MB free hard disk space • Native Microsoft TCP/IP communication protocol • Native Microsoft PPP dialer for dial-up connections • Ethernet NIC for network connections • Wireless adapter for wireless network connections • Adobe Acrobat Reader for documentation • MSI installer 3.0 or later.

Operating system support	Minimum system requirements
• Mac OS X v10.9 Mavericks • Mac OS X v10.10 Yosemite • Mac OS X v10.11 El Capitan • Mac OS X v10.12 Sierra	• Apple Mac computer with an Intel processor • 256 MB of RAM • 20 MB of hard disk drive (HDD) space • TCP/IP communication protocol • Ethernet NIC for network connections • Wireless adapter for wireless network connections

For Microsoft Windows servers, the AntiVirus and Vulnerability Scan features for FortiClient are supported.

Licensing

FortiClient in standalone mode does not require a license.

FortiClient in managed mode requires a license. In managed mode, FortiClient licensing is applied to FortiGate or EMS.

When using the ten (10) free licenses for FortiClient in managed mode, support is provided on the Fortinet Forums (forum.fortinet.com). Phone support is not provided when using the free licenses. Phone support is provided for paid licenses.

FortiClient licenses for FortiGate

FortiGate 30 series and higher models include a FortiClient license for ten (10) free connected endpoints. For additional connected endpoints, you must purchase a FortiClient license subscription. Contact your Fortinet sales representative for information about FortiClient licenses.

For a video about applying FortiClient licenses to FortiGate, see the *How to Purchase or Renew FortiClient Endpoint Subscription* video at https://video.fortinet.com/product/forticlient.

FortiClient licenses for EMS

EMS includes a FortiClient license for ten (10) free connected endpoints for evaluation. For additional connected endpoints, you must purchase a FortiClient license subscription. Contact your Fortinet sales representative for information about FortiClient licenses.

For a video about applying FortiClient licenses to EMS, see the *How to License FortiClient EMS* video at https://video.fortinet.com/product/forticlient-ems.

FortiClient setup types and modules

The Advanced Persistent Threat (APT) module is available only for FortiClient (Windows).

When you install FortiClient, you can choose which setup type and modules to install:

- Security Fabric Agent
- Secure Remote Access
- Advanced Persistent Threat (APT) Components
- Additional Security Features

The following table summarizes the impact of the options:

Setup type	Description	Impact on FortiClient Console
Security Fabric Agent	Enabled by default and installs components to support the Security Fabric that is available with FortiGate, including FortiClient Telemetry, vulnerability scanning, and vulnerability remediation.	Displays the following tabs: • *Compliance* • *Vulnerability Scan*
Secure Remote Access	Optional. Supports SSL and IPsec VPN access.	Displays the *Remote Access* tab.
Advanced Persistent Threat (APT) Components	Optional. Supports FortiSandbox.	Displays the *Sandbox Detection* tab to let you connect to a FortiSandbox unit.
Additional Security Features	Optional. Supports AntiVirus, Web Filtering, Application Firewall, and Single Sign On. You can select one, more, or all security features.	Displays the following tabs when all security features are selected: • *AntiVirus* • *Web Filtering* • *Application Firewall* When *Single Sign On* is selected, FortiClient supports the single sign on feature. When a security feature is not selected, the tab is hidden from view in FortiClient Console.

EMS and FortiClient setups

For FortiClient in managed mode, you can use an EMS profile to disable installed components in FortiClient Console but you cannot use an EMS profile to enable uninstalled components in FortiClient Console. See EMS and endpoint profiles on page 23.

For example, if you install FortiClient with APT components selected, the *Sandbox Detection* tab is included in FortiClient Console, and you can use an EMS profile to disable the *Sandbox Detection* tab. However, if you install FortiClient with APT components cleared, the *Sandbox Detection* tab is excluded from FortiClient Console and you cannot use an EMS profile to enable the *Sandbox Detection* tab.

FortiGate compliance and FortiClient setups

For endpoints that will have FortiClient Telemetry connected to FortiGate with endpoint compliance enabled, ensure FortiClient is installed with the setup required by the FortiGate compliance rules. See Compliance rules on page 22.

For example, if the FortiGate compliance rules require the *Web Filter* tab to be enabled in FortiClient Console, FortiClient must be installed with *Additional Features* and *Web Filtering* selected to meet the compliance rules. If FortiClient is installed with an incorrect setup for the compliance rules, you must uninstall FortiClient and reinstall FortiClient with the setup required by the compliance rules.

Firmware images and tools

Firmware images and tools are available for Microsoft Windows and Mac OS X. See Custom FortiClient installation files and rebranding on page 32.

Microsoft Windows

The following files are available in the firmware image file folder:

- FortiClientSetup_5.6.xx.xxxx.exe
  Standard installer for Microsoft Windows (32-bit).
- FortiClientSetup_5.6.xx.xxxx.zip
  A zip package containing FortiClient.msi and language transforms for Microsoft Windows (32-bit). Some properties of the MSI package can be customized with FortiClient Configurator tool.
- FortiClientSetup_5.6.xx.xxxx_x64.exe
  Standard installer for Microsoft Windows (64-bit).
- FortiClientSetup_5.6.xx.xxxx_x64.zip
  A zip package containing FortiClient.msi and language transforms for Microsoft Windows (64-bit). Some properties of the MSI package can be customized with FortiClient Configurator tool.
- FortiClientTools_5.6.xx.xxxx.zip
  A zip package containing miscellaneous tools, including VPN Automation files:

The following tools and files are available in the FortiClientTools_5.6.xx.xxxx.zip file:

- FortiClientVirusCleaner
  A virus cleaner.
- OnlineInstaller
  This file downloads and installs the latest FortiClient file from the public FDS.
- SSLVPNcmdline
  Command line SSL VPN client.
- SupportUtils
  Includes diagnostic, uninstallation, and reinstallation tools.
- VPNAutomation
  A VPN automation tool.

Mac OS X

The following files are available in the firmware image file folder:

- FortiClient_5.6.x.xxx_macosx.dmg
  Standard installer for Mac OS X.
- FortiClientTools_5.6.x.xxx_macosx.tar
  FortiClient includes various utility tools and files to help with installations.

The following file is available in the FortiClientTools `.tar` file:

- OnlineInstaller
  This file downloads and installs the latest FortiClient file from the public FDS.

Where to download FortiClient installation files

You can download the FortiClient installation files from the following sites:

- Fortinet Customer Service & Support: https://support.fortinet.com
  Requires a support account with a valid support contract. Download the Microsoft Windows (32-bit/64-bit) or the Mac OS X installation file.
- FortiClient homepage: www.forticlient.com
  Download the FortiClient online installation file. The installer file performs a virus and malware scan of the target system prior to installing FortiClient.

Custom FortiClient installation files and rebranding

The following tools are available from Fortinet Developer Network at https://fndn.fortinet.net/:

- FortiClient Configurator Tool
- FortiClient Rebranding Tool

An account is required to access the Fortinet Developer Network. Information about creating an account is available at https://fndn.fortinet.net/

You can use the free FortiClient Configurator Tool to create customized FortiClient installation files, and you can use the licensed FortiClient Rebranding Tool to create customized FortiClient Installation file and rebrand FortiClient.

Starting with FortiClient 5.6.0, the FortiClient Configurator Tool is available for free download from the *Tools* > *Personal Toolkit* section of FNDN at https://fndn.fortinet.net/.

Provisioning

FortiClient can be installed on a standalone computer using the installation wizard or deployed to multiple Microsoft Windows systems using Microsoft Active Directory (AD).

You can use EMS to deploy FortiClient to multiple Microsoft Windows systems. See the *FortiClient EMS Administration Guide*.

Installing FortiClient on computers

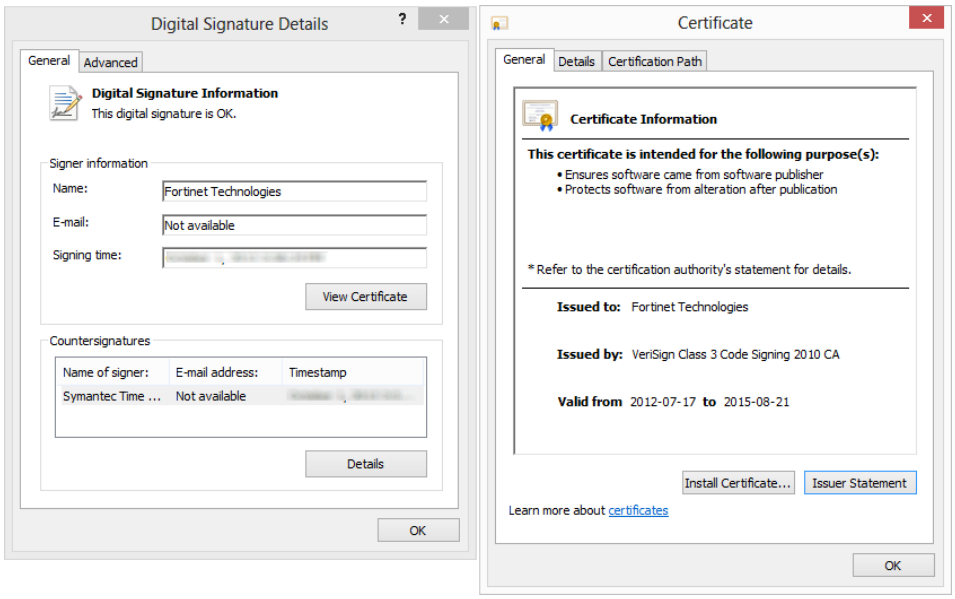
The following section describes how to install FortiClient on a computer running a Microsoft Windows or Mac OS X operating system.

Microsoft Windows computer

The following instructions guide you though the installation of FortiClient on a Microsoft Windows computer. For more information, see the *FortiClient (Windows) Release Notes*.

When installing FortiClient, it is recommended to use the FortiClientOnlineInstaller file. This file launches the FortiClient Virus Cleaner which scans the target system prior to installing the FortiClient application. The FortiClientOnlineInstaller file always installs the latest version of FortiClient that available on FDN, not the version of FortiClient referenced in the filename or listed on the Customer Service & Support site.

To check the digital signature of FortiClient, right-click the installation file and select *Properties*. In this menu you can set file attributes, run the compatibility troubleshooter, view the digital signature and certificate, install the certificate, set file permissions, and view file details.

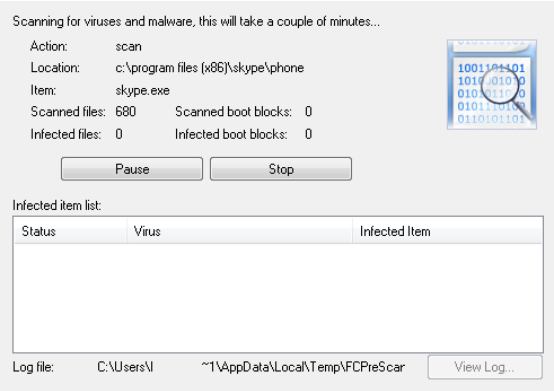


To install FortiClient (Windows):

1. Double-click the FortiClient executable file. The *Setup Wizard* launches.

   When using the FortiClientOnlineInstaller file, the FortiClient Virus Cleaner runs before launching the *Setup Wizard*.

   If a virus is found that prevents the infected system from downloading the new FortiClient package, see Installing FortiClient on infected systems on page 38.



2. In the *Welcome to the FortiClient Setup Wizard* screen, perform the following actions:
   a. Click the *License Agreement* button, and read the license agreement. You have the option to print the EULA in this License Agreement screen. Click *Close* to return to the installation wizard.
   b. Select the *Yes, I have read and accept the license* checkbox.
3. Click *Next* to continue.

   The *Choose Setup Type* screen displays.
4. Select one or more of the following setup types:

   The *Security Fabric Agent* option is enabled by default, and you cannot deselect it. See FortiClient setup types and modules on page 30.

- *Security Fabric Agent*: Endpoint telemetry, host vulnerability scanning and remediation
- *Secure Remote Access*: VPN components (IPsec and SSL) will be installed
- *Advanced Persistent Threat (APT) Components*: FortiSandbox detection and quarantine features
- *Additional Security Features*: AntiVirus, Web Filtering, Single Sign On, Application Firewall

5. Click *Next* to continue.
   The *Destination Folder* screen displays.
6. (Optional) Click *Change* to choose an alternate folder destination for installation.
7. Click *Next* to continue.
   FortiClient searches the target system for other installed antivirus software. If found, FortiClient displays the *Conflicting Antivirus Software* page. You can exit the current installation and uninstall the antivirus software, disable the antivirus feature of the conflicting software, or continue with the installation with FortiClient realtime protection disabled.

This dialog box displays during a new installation of FortiClient and when upgrading from an older version of FortiClient, which does not have the antivirus feature installed.

It is recommended to uninstall the conflicting antivirus software before installing FortiClient or enabling the antivirus realtime protection feature. Alternatively, you can disable the antivirus feature of the conflicting software.

8. Click *Next* to continue.
   The *Ready to install FortiClient* screen displays.
9. Click *Install* to begin the installation.
10. Click *Finish* to exit the FortiClient Setup Wizard.
    On a new FortiClient installation, you do not need to reboot your system. When upgrading the FortiClient version, you must restart your system for the configuration changes made to FortiClient to take effect. Select *Yes* to restart your system now or select *No* to manually restart later.
    FortiClient updates signatures and components from the FortiGuard Distribution Network (FDN).
11. FortiClient attempts to connect FortiClient Telemetry to the FortiGate.
    If the FortiGate cannot be located on the network, manually connect FortiClient Telemetry. See Connecting FortiClient Telemetry manually on page 49.

If you have any questions about connecting FortiClient Telemetry to FortiGate, contact your network administrator.

12. To launch FortiClient, double-click the desktop shortcut icon.

Microsoft Server

You can install FortiClient on a Microsoft Windows Server 2008 R2, 2012, or 2012 R2 server. You can use the regular FortiClient Windows image for Server installations.

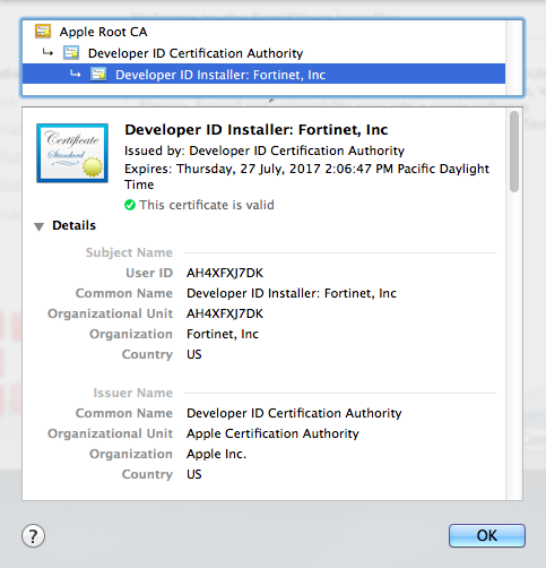
Refer to the Microsoft knowledge base for caveats on installing antivirus software in a server environment. See the Microsoft Anti-Virus exclusion list: http://social.technet.microsoft.com/wiki/contents/articles/953.microsoft-anti-virus-exclusion-list.aspx

Mac OS X computer

The following instructions will guide you though the installation of FortiClient on a Mac OS X computer. For more information, see the *FortiClient (Mac OS X) Release Notes*.

To install FortiClient (Mac OS X):

1. Double-click the FortiClient `.dmg` installer file. The *FortiClient for Mac OS X* dialog box displays.
2. Double-click *Install*. The *Welcome to the FortiClient Installer* dialog box displays.
3. (Optional) Click the lock icon in the upper-right corner to view certificate details and click *OK* to close the dialog box.



4. Click *Continue*.
5. Read the Software License Agreement and click *Continue*.

   You have the option to print or save the Software Agreement in this window. You are prompted to *Agree* with the terms of the license agreement.
6. If you agree with the terms of the license agreement, click *Agree* to continue the installation.
7. Perform one of the following actions:
   - Click *Install* to perform a standard installation on this computer, which includes the following modules: Security Fabric Agent and Secure Remote Access.
   - Click *Customize* to choose which FortiClient modules to install. See FortiClient setup types and modules on page 30.
8. Depending on your system, you may be prompted to enter your system password.
9. After the installation completes successfully, Click *Close* to exit the installer.

   FortiClient has been saved to the *Applications* folder.

10. Double-click the FortiClient icon to launch the application. The application console loads to your desktop. Click the lock icon in FortiClient Console to make changes to the FortiClient configuration.

Installing FortiClient on infected systems

The FortiClient installer always runs a quick antivirus scan on the target host system before proceeding with the complete installation. If the system is clean, installation proceeds as usual.

Any virus found during this step is quarantined before installation continues.

In case a virus on an infected system prevents downloading of the new FortiClient package, use the following process:

- Boot into “safe mode with networking” (which is required for the FortiClient installer to download the latest signature packages from the Fortinet Distribution Network).
- Run the FortiClient installer.

This scans the entire file system. A log file is generated in the logs sub-directory. If a virus is found, it is quarantined. When complete, reboot back into normal mode and run the FortiClient installer to complete the installation.

Microsoft Windows will not allow FortiClient installation to complete in safe mode. An error message is generated. It is necessary to reboot back into normal mode to complete the installation.

Installing FortiClient as part of cloned disk images

If you configure computers using a cloned hard disk image, you need to remove the unique identifier from the FortiClient application. You will encounter problems with FortiGate if you deploy multiple FortiClient applications with the same identifier.

This section describes how to include a custom FortiClient installation in a cloned hard disk image but remove its unique identifier. On each computer configured with the cloned hard disk image, the FortiClient application will generate its own unique identifier the first time the computer is started.

To include a FortiClient installation in a hard disk image:

1. Install and configure the FortiClient application to suit your requirements.
   You can use a standard or a customized installation package.
2. Right-click the FortiClient icon in the system tray and select *Shutdown FortiClient*.
3. From the folder where you expanded the FortiClientTools.zip file, run RemoveFCTID.exe. The RemoveFCTID tool requires administrative rights.

Do not include the RemoveFCTID tool as part of a logon script.

4. Shut down the computer.

Do not reboot the Windows operating system on the computer before you create the hard disk image. The FortiClient identifier is created before you log on.

5. Create the hard disk image and deploy it as needed.

Installing FortiClient using the CLI

You can install FortiClient using the CLI. The following table summarizes the installation options available when using the CLI.

Option	Description
`/extract "<Directory>"`	Extracts all installation packages to the specified directory.
`/msicl "[PROPERTY=PropertyValue]..."` or `/v"[PROPERTY=PropertyValue]..."`	Properties to set for installation.
`/lang<LCID>`	Enter the locale ID of the transform to apply to the installation.
`/quiet`	Installation is in quiet mode and requires no user interaction.
`/passive`	Installation is in unattended mode, showing only the progress bar.
`/norestart`	Does not restart the machine after installation is complete.
`/promptrestart`	Prompts the user to restart the machine if necessary.
`/forcerestart`	Always restarts the machine after installation.
`/uninstall`	Uninstalls FortiClient.
`/log"<LogFile>"`	Creates a log file with the specified name.

The following example installs FortiClient build 1131 in quiet mode, creating a log file with the name "Log":

```
FortiClientSetup_5.6.4.1131_x64.exe /quiet /log"Log"
```

Deploying FortiClient using Microsoft AD servers

There are multiple ways to deploy FortiClient MSI packages to endpoints including using Microsoft Active Directory (AD). See Firmware images and tools on page 31.

The following instructions are based on Microsoft Windows Server 2008. If you are using a different version of Microsoft Server, your MMC or snap-in locations may be different.

Using Microsoft AD to deploy FortiClient

To use Microsoft AD to deploy FortiClient:

1. On your domain controller, create a distribution point.
2. Log on to the server computer as an administrator.
3. Create a shared network folder where the FortiClient MSI installer file will be distributed from.
4. Set file permissions on the share to allow access to the distribution package. Copy the FortiClient MSI installer package into this share folder.
5. Select *Start* > *Administrative Tools* > *Active Directory Users and Computers*.
6. After selecting your domain, right-click to select a new Organizational Unit (OU).
7. Move all the computers you wish to distribute the FortiClient software to into the newly-created OU.
8. Select *Start* > *Administrative Tools* > *Group Policy Management*. The Group Policy Management MMC Snap-in opens. Select the OU you just created. Right-click it, *Select Create a GPO* in this domain, and link it here. Give the new GPO a name then select *OK*.
9. Expand the Group Policy Object container and find the GPO you just created. Right-click the GPO and select *Edit*. The Group Policy Management Editor MMC Snap-in opens.
10. Expand *Computer Configuration* > *Policies* > *Software Settings*. Right-click *Software Settings* and select *New* > *Package*.
11. Select the path of your distribution point and FortiClient installer file and then select *Open*. Select *Assigned* and select *OK*. The package is then generated.
12. If you wish to expedite the installation process, on the server and client computers, force a GPO update.
13. The software is installed on the client computer's next reboot. You can also wait for the client computer to poll the domain controller for GPO changes and install the software then.

Using Microsoft AD to uninstall FortiClient

To use Microsoft AD to uninstall FortiClient:

1. On your domain controller, select *Start* > *Administrative Tools* > *Group Policy Management*. The Group Policy Management MMC Snap-in opens. Expand the Group Policy Objects container and right-click the Group Policy Object you created to install FortiClient and select *Edit*. The *Group Policy Management Editor* opens.
2. Select *Computer Configuration* > *Policy* > *Software Settings* > *Software Installation*. You will now be able to see the package used to install FortiClient.
3. Right-click the package and select *All Tasks* > *Remove*. Choose *Immediately* to uninstall the software from users and computers, or *Allow* users to continue to use the software but prevent new installations. Select *OK*. The package deletes.
4. If you wish to expedite the uninstall process on both the server and client computers, force a GPO update as shown in the previous section. The software is uninstalled on the client computer's next reboot. You can also wait for the client computer to poll the domain controller for GPO changes and uninstall the software then.

Deploying FortiClient using Microsoft AD user groups

When FortiClient Telemetry connects to FortiGate, the user's AD domain name and group are sent to FortiGate. Administrators may configure FortiGate to deploy endpoint and/or firewall profiles based on the end user's AD domain group.

The following steps are discussed in more detail:

- Configuring users and groups on AD servers
- Configuring FortiAuthenticator
- Configuring FortiGate
- Connecting FortiClient Telemetry to FortiGate
- Monitoring FortiClient connections

Configuring users and groups on AD servers

Create the user accounts and groups on the AD server. Groups may have any number of users. A user may belong to more than one group at the same time.

Configuring FortiAuthenticator

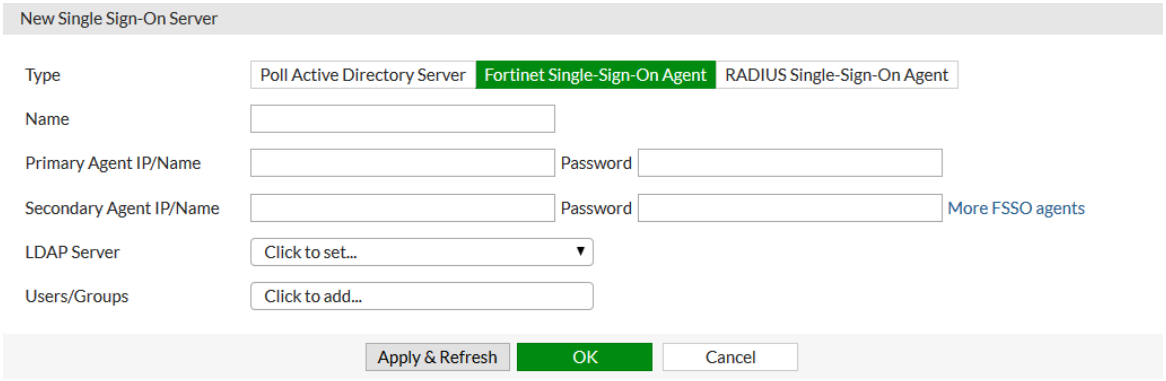
Configure FortiAuthenticator to use the AD server you created. See the *FortiAuthenticator Administration Guide* in the Fortinet Document Library.

Configuring FortiGate

FortiGate

Add the FortiAuthenticator or Fortinet Single Sign-On Agent (FSSO):

1. Go to *User & Device* > *Single Sign-On*.
2. Select *Create New* in the toolbar. The *New Single Sign-On Server* window opens.



3. In the type field, select *Fortinet Single-Sign-On Agent*.

4. Enter the information required for the agent. This includes the name, primary and secondary IP addresses, and passwords. Select an LDAP server in the dropdown list if applicable. Select *More FSSO agents* to add up to three additional agents.
5. Select *OK* to save the agent configuration.

Create a user group:

1. Go to *User & Device* > *User Groups*.
2. Select *Create New* in the toolbar. The *New User Group* window opens.
3. In the type field, select *Fortinet Single-Sign-On (FSSO)*.
4. Select members from the dropdown list.
5. Select *OK* to save the group configuration.

Configure the FortiClient profile:

1. Go to *Security Profiles* > *FortiClient Profiles*.
2. Select *Create New* in the toolbar. The *New FortiClient Profile* window opens.
3. Enter a profile name and optional comments.
4. In the *Assign Profile To* dropdown list select the FSSO user group(s).
5. Configure FortiClient configuration as required.
6. Select *OK* to save the new FortiClient profile.

Create any number of FortiClient profiles with different groups and different settings. The default profile will be assigned to users who connect successfully, but have no matching FortiClient profile.

Configure the firewall policy:

Configure the firewall policy. Ensure *Compliant with FortiClient Profile* is selected in the policy.

Connecting FortiClient Telemetry to FortiGate

The Microsoft Windows system where FortiClient is installed should join the domain of the AD server configured earlier. Users may log in with their domain username.

Following this, endpoint connections send the logged-in user's name and domain to the FortiGate. The FortiGate will assign the appropriate profiles based on the configurations.

Monitoring FortiClient connections

The following FortiOS CLI command lists information about connected clients. This includes domain-related details for the client if any.

```
diagnose endpoint record-list
   Record #1:
      IP_Address = 172.172.172.111(1)
      MAC_Address = b0:ac:6f:70:e0:a0
```

```
Host MAC_Address = b0:ac:6f:70:e0:a0
MAC list = b0-ac-6f-70-e0-a0;
VDOM = root
Registration status: Forticlient installed but not registered
Online status: offline
DHCP on-net status: off-net
DHCP server: None
FCC connection handle: 6
FortiClient version: 5.1.29
AVDB version: 22.137
FortiClient app signature version: 3.0
FortiClient vulnerability scan engine version: 1.258
FortiClient feature version status: 0
FortiClient UID: BE6B76C509DB4CF3A8CB942AED2064A0 (0)
FortiClient config dirty: 1:1:1
FortiClient KA interval dirty: 0
FortiClient Full KA interval dirty: 0
FortiClient server config: d9f86534f03fbed109676ee49f6cfc09::
FortiClient config: 1
FortiClient iOS server mconf:
FortiClient iOS mconf:
FortiClient iOS server ipsec_vpn mconf:
FortiClient iOS ipsec_vpn mconf:
Endpoint Profile: Documentation
Reg record pos: 0
Auth_AD_groups:
Auth_group:
Auth_user:
Host_Name:
OS_Version: Microsoft Windows 7 , 64-bit Service Pack 1 (build 7601)
Host_Description: AT/AT COMPATIBLE
Domain:
Last_Login_User: FortiClient_User_Name
Host_Model: Studio 1558
Host_Manufacturer: Dell Inc.
CPU_Model: Intel(R) Core(TM) i7 CPU Q 720 @ 1.60GHz
Memory_Size: 6144
Installed features: 55
Enabled features: 21
online records: 0; offline records: 1
status -- none: 0; uninstalled: 0; unregistered: 1; registered: 0; blocked: 0
```

Upgrading FortiClient

For information about supported upgrade paths for FortiClient, see the *FortiClient Release Notes*.

For FortiClient in managed mode, an administrator may control FortiClient upgrades for you, and you may be unable to manually upgrade FortiClient. See also EMS and automatic upgrade of FortiClient on page 26.

During a FortiClient upgrade to 5.6.4, FortiClient installs the same features that were previously installed. If you want to install different features, you must uninstall the previous version of FortiClient, and install FortiClient 5.6.4 with the desired features.

For FortiClient in managed mode, when an administrator deploys a FortiClient upgrade from EMS to endpoints running a Windows operating system, an *Upgrade Schedule* dialog box displays in advance on the endpoint to let endpoint users schedule the upgrade and mandatory endpoint reboot. If no FortiClient is installed on the endpoint, no reboot is required for the installation, and no *Upgrade Schedule* dialog box displays. The endpoint user can postpone the reboot for a maximum of 24 hours. Before the mandatory reboot occurs, a FortiClient dialog box displays with a 15 minute warning.

To upgrade FortiClient:

1. Go to *Help* > *About*.
2. Beside the version, click *Update Available: <version number>*.

To upgrade FortiClient from FortiTray:

1. Select the Windows System Tray.
2. Right-click the *FortiTray* icon, and select *Update Available: <version number>*.

FortiClient Telemetry

In managed mode, FortiClient uses a gateway IP address to connect FortiClient Telemetry to FortiGate or EMS.

When your administrator has configured FortiGate for network access control (NAC), you must connect FortiClient Telemetry to FortiGate to access the network, and you must also maintain a compliant status to retain access to the network. See Compliance on page 49.

For information about creating Telemetry gateway IP lists, see Telemetry gateway IP lists on page 26.

This section applies only to FortiClient in managed mode.

Telemetry data

When FortiClient Telemetry is connected to FortiGate and/or EMS, the following data about the endpoint and its workload is collected and sent to FortiGate and/or EMS:

- Hardware information, such as MAC addresses
- Software information, such as the version of operating system on the endpoint
- Identification information, such as user name, user picture, and host name
- Vulnerability information reported by the vulnerability scanning module

When FortiClient Telemetry is connected to FortiGate, the Security Fabric uses the information to understand the endpoint and its workload to better protect it.

How FortiClient locates FortiGate or EMS

FortiClient uses the following methods in the following order to locate FortiGate or EMS for Telemetry connection:

- Manually entering the gateway IP address, which means the endpoint user enters the gateway IP address of FortiGate or EMS into FortiClient Console. See Connecting FortiClient Telemetry manually on page 49.
- Telemetry Gateway IP list

  FortiClient Telemetry searches for IP addresses in its subnet in the gateway IP list. It connects to the FortiGate in the list that is also in the same subnet as the host system.

  If FortiClient cannot find any FortiGates in its subnet, it attempts to connect to the first reachable FortiGate in the list, starting from the top. The order of the list is maintained as configured in the gateway IP list.
- Default gateway IP address

  The default gateway IP address is specified on the FortiClient endpoint and is used to automatically connect to FortiGate. This method does not support connection to EMS.

FortiClient obtains the default gateway IP address from the operating system on the endpoint. The default gateway IP address of the endpoint should be the IP address for the FortiGate interface with Telemetry enabled.

- VPN
- Remembered gateway IP list

  You can configure FortiClient to remember gateway IP addresses when you connect Telemetry to FortiGate or EMS. Later FortiClient can use the remembered IP addresses to automatically connect Telemetry to FortiGate or EMS.

FortiClient uses the same process to connect Telemetry to FortiGate or EMS after the FortiClient endpoint reboots, rejoins the network, or encounters a network change.

Connecting FortiClient Telemetry after installation

After FortiClient software installation completes on an endpoint, FortiClient automatically launches and searches for FortiGate or EMS to connect FortiClient Telemetry. See How FortiClient locates FortiGate or EMS on page 45.

To connect FortiClient Telemetry after installation:

1. When FortiClient locates a FortiGate or EMS, the *FortiGate Detected* or *Enterprise Management Server (EMS) Detected* dialog box displays.

   Following is an example of the *FortiGate Detected* dialog box:

   Following is an example of the *Enterprise Management Server (EMS) Detected* dialog box:

The following options are available:

Endpoint User	Displays the name of the endpoint user logged into the endpoint.
Logged into Domain	Displays the domain name if applicable.
Hostname	Displays the endpoint name.
Profile Details	Available only when EMS is detected. Click to display details of the profile that FortiClient will receive after you accept connection to EMS. See EMS and endpoint profiles on page 23.
Remember this FortiGate	Available only when FortiGate is detected. Select this checkbox for FortiClient to remember the gateway IP address of the FortiGate to which you are connecting Telemetry. See Remembering gateway IP addresses on page 47.
Remember this Server	Available only when EMS is detected. Select for FortiClient to remember the gateway IP address of the EMS to which you are connecting Telemetry. See Remembering gateway IP addresses on page 47.

2. Click *Accept* to connect FortiClient Telemetry to the identified FortiGate or EMS.

   Alternately, you can click *Cancel* to launch FortiClient software without connecting FortiClient Telemetry. FortiClient launches in standalone mode. You can manually connect FortiClient Telemetry later.

   After FortiClient Telemetry is connected to FortiGate or EMS, FortiClient receives compliance rules from FortiGate and/or a profile from EMS. A system tray bubble message displays once the download is complete.

Remembering gateway IP addresses

When you confirm Telemetry connection to FortiGate or EMS, you can instruct FortiClient to remember the gateway IP address of the FortiGate or EMS. If a connection key is required, FortiClient remembers the connection password too. FortiClient can remember up to 20 gateway IP addresses for FortiGate and EMS.

The remembered IP addresses display in the local gateway IP list. FortiClient can use the remembered gateway IP addresses to automatically connect to FortiGate or EMS.

See Forgetting gateway IP addresses on page 59.

To remember IP addresses for FortiGate or EMS:

1. In the *FortiGate or EMS Detected* dialog box, select the *Remember this FortiGate* or *Remember this EMS* (not shown) checkbox.

2. Click *Accept*.

   FortiClient remembers the IP address and password, if applicable.

Compliance

The *Compliance* tab displays whether FortiClient Telemetry is connected to FortiGate or EMS. You can use the *Compliance* tab to manually connect FortiClient Telemetry to FortiGate or EMS and to disconnect FortiClient Telemetry from FortiGate or EMS.

When FortiClient Telemetry is connected to FortiGate and endpoint control is enabled by the FortiGate administrator, the *Compliance* tab displays whether FortiClient and the endpoint are compliant with the FortiGate compliance rules and provides information about maintaining a compliant endpoint.

Enabling compliance

For FortiClient in standalone mode, the *Compliance* tab is visible, but not used.

For FortiClient in managed mode, an administrator enables and configures the *Compliance* tab by using FortiOS.

Connecting FortiClient Telemetry manually

FortiClient Telemetry must be connected to FortiGate to use the compliance feature. Alternately, FortiClient Telemetry can be connected to EMS, but you cannot use the compliance feature when the FortiClient Telemetry is connected to EMS. See also Telemetry connection options on page 24.

If FortiClient Telemetry was not automatically connected after FortiClient installation, you can manually connect FortiClient Telemetry to FortiGate or EMS.

To manually connect FortiClient Telemetry to FortiGate:

1. Go to the *Compliance* tab.
2. In the *FortiGate or EMS* box, type the IP address or FQDN of FortiGate, and click *Connect*.
   FortiClient Telemetry connects to FortiGate, and FortiClient receives a profile of compliance rules from FortiGate.

To manually connect FortiClient Telemetry to EMS:

1. Go to the *Compliance* tab.
2. In the *FortiGate or EMS* box, type the IP address or FQDN of EMS, and click *Connect*.
   FortiClient Telemetry connects to EMS, and FortiClient receives a profile of configuration information from EMS.

To manually connect FortiClient Telemetry to FortiGate and EMS:

1. Go to the *Compliance* tab.
2. In the *FortiGate or EMS* box, type the IP address or FQDN of FortiGate, and click *Connect*.
   FortiClient Telemetry establishes the primary connection to FortiGate, and FortiClient receives a profile of compliance rules from FortiGate. FortiClient Telemetry also automatically establishes a secondary connection to EMS, and FortiClient receives a profile of configuration information from EMS.

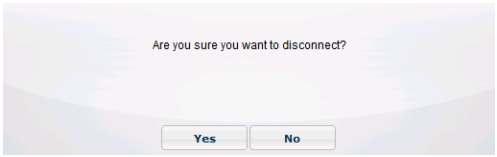
Disconnecting FortiClient Telemetry

You must disconnect FortiClient Telemetry from FortiGate or EMS to connect to another FortiGate or EMS or to disable and uninstall FortiClient.

When FortiClient Telemetry is connected to EMS, an EMS administrator may disconnect FortiClient for you. This is sometimes referred to as deregistering FortiClient. When an EMS administrator disconnects FortiClient Telemetry for you, the Telemetry Gateway list is also removed from FortiClient. See Viewing gateway IP lists on page 58.

To disconnect FortiClient Telemetry:

1. On the *Compliance* tab, click the *Click to Disconnect* link. A confirmation dialog box displays.



2. Click *Yes* to disconnect FortiClient Telemetry from FortiGate or EMS.

After you disconnect FortiClient Telemetry from FortiGate or EMS, FortiClient Telemetry automatically connects with the FortiGate or EMS when you rejoin the network. See Forgetting gateway IP addresses on page 59.

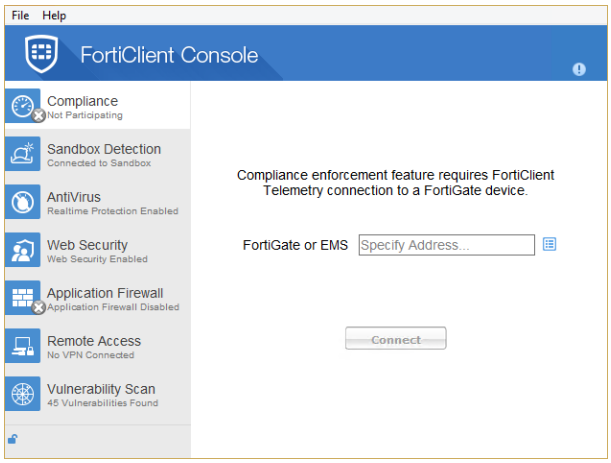
Viewing compliance status

Information available on the *Compliance* tab depends on whether FortiClient is running in standalone mode or managed mode. In managed mode, the information displayed on the *Compliance* tab also depends on whether FortiClient Telemetry is connected to FortiGate or EMS.

Standalone mode

When FortiClient is running in standalone mode, the *Compliance* tab is visible, but not used. The *Compliance* tab is labeled *Not Participating*.

If you want to use the compliance feature, you must connect FortiClient Telemetry to FortiGate.

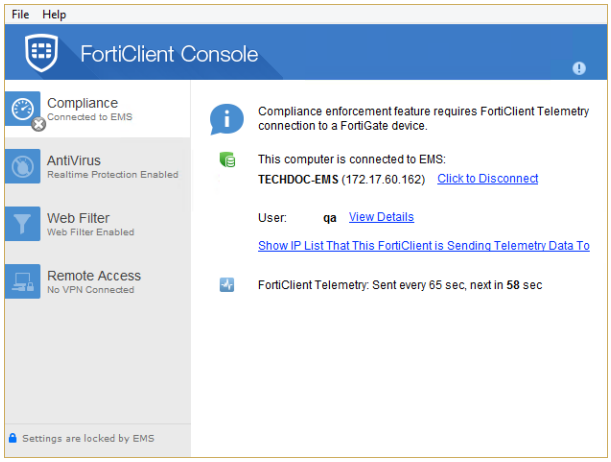


The *Compliance* tab displays the following information:

FortiGate or EMS	Type the IP address or FQDN of FortiGate or EMS, and click *Connect* to connect FortiClient Telemetry.
Show IP List that this FortiClient is sending Telemetry data to	Click the icon to display the list of gateway IP addresses. You can click an IP address in the list to populate the *FortiGate IP* box.
Unlocked icon	Indicates the settings in FortiClient Console are unlocked, and endpoint users can change them.
Connect	Click to connect to FortiGate or EMS after populating the *FortiGate or EMS* box with an IP address.

Managed mode with EMS

When FortiClient Telemetry is connected to EMS, compliance is not enforced. The *Compliance* tab is labeled *Connected to EMS*.



The *Compliance* tab displays the following information:

Compliance information		Indicates the compliance enforcement feature requires FortiClient Telemetry connection to FortiGate.
EMS information		Displays the name and IP address of the EMS to which FortiClient Telemetry is connected. You can disconnect by clicking the *Click to Disconnect* link. Displays the name of the user logged into the endpoint. See also Accessing endpoint details on page 54. Click the *Show IP List That This FortiClient is Sending Telemetry Data To* link to view the gateway IP list being used for FortiClient Telemetry connection.
FortiClient Telemetry information		Displays how often FortiClient Telemetry communicates with FortiClient EMS and when the next communication will occur. FortiClient Telemetry communicates information between FortiClient and EMS.
Locked icon		Indicates EMS has locked the settings in FortiClient Console, and endpoint users cannot change them.

Managed mode with FortiGate

When FortiClient Telemetry is connected to FortiGate and the FortiGate administrator has disabled compliance, network access compliance (NAC) is not enforced. The *Compliance* tab displays *Not Participating* and you are not required to maintain a compliant status to access the network.

When FortiClient Telemetry is connected to FortiGate and the FortiGate administrator has enabled compliance, NAC is enforced and you may be required to maintain a compliant status to access the network, depending on how FortiGate enforces NAC.

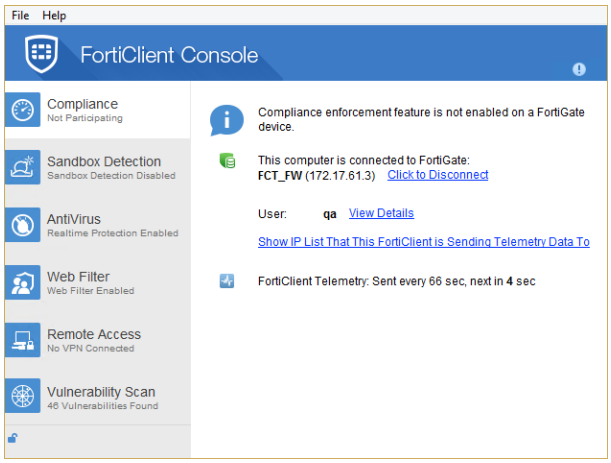
If FortiGate is configured to block network access for endpoints with non-compliant status, the following requirements must be met to maintain a compliant status and network access:

- FortiClient must be installed on endpoints.
- FortiClient Telemetry must be connected to FortiGate for the endpoint to receive a profile from FortiGate that contains the compliance rules.
- FortiClient software and endpoint must be configured as specified by the FortiGate compliance rules.

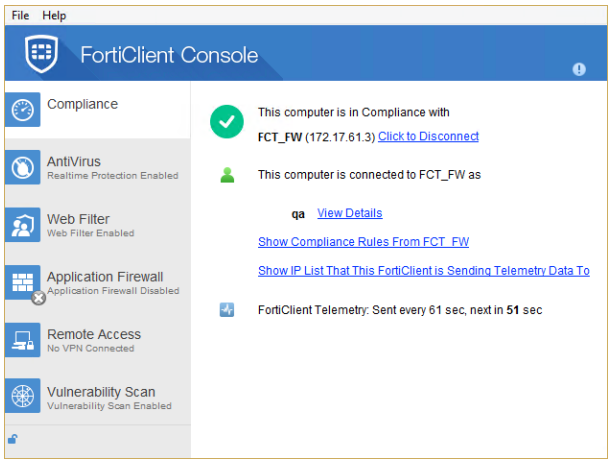
When FortiGate is integrated with EMS, the endpoint may also receive a profile from EMS that contains FortiClient configuration information.

If FortiGate is configured to warn endpoints about non-compliant status, you can acknowledge the status and access the network without fixing the issues causing a non-compliant status.

The following dialog box shows an example of an endpoint connected to a FortiGate with the compliance feature disabled.



The following dialog box shows an example of an endpoint connected to a FortiGate with the compliance feature enabled, and the endpoint is in compliance with the FortiGate compliance rules.



The *Compliance* tab displays the following information:

Compliance		Indicates the endpoint compliance feature is enabled on FortiGate and the endpoint is in compliance with FortiGate compliance rules. See Fixing not compliant (blocked) on page 60 and Fixing not compliant (warning) on page 64.
		Indicates the compliance enforcement feature is not enabled on FortiGate.
FortiGate information		Displays the name and IP address of the FortiGate to which FortiClient Telemetry is connected. You can disconnect by clicking the *Click to Disconnect* link.

User information		Displays the name of the user logged into the endpoint. See Accessing endpoint details on page 54. Click the *Show Compliance Rules from <FortiGate>* link to display the compliance rules for FortiGate. Click the *Show IP List That This FortiClient is Sending Telemetry Data To* link to view the gateway IP list being used for FortiClient Telemetry connection.
FortiClient Telemetry information		Displays how often FortiClient Telemetry communicates with FortiGate and when the next communication will occur. FortiClient Telemetry communicates information between FortiClient and FortiGate, sending status information to FortiGate and receiving network access rules from FortiGate. When FortiGate is integrated with EMS, notification information is also sent to EMS. EMS may also send endpoint profiles of configuration information to FortiClient.
Managed		Displays the name of EMS if EMS is managing the endpoint.
Locked icon		Indicates EMS has locked the settings in FortiClient Console and you cannot change them.
Unlocked icon		Indicates the settings in FortiClient Console are unlocked and endpoint users can change them.

Accessing endpoint details

When FortiClient is in managed mode, you can access details on the *Compliance* tab about the logged in user, the endpoint, and FortiGate or EMS.

Viewing user details

You can view details about the logged in user when FortiClient Telemetry is connected to FortiGate or EMS.

You cannot view user details when FortiClient is not compliant with FortiGate rules.

When an administrator configures FortiClient to send logs to FortiAnalyzer or FortiManager, some user details are visible in FortiAnalyzer, FortiManager, and FortiOS. See Sending logs to FortiAnalyzer or FortiManager on page 131.

To view user details:

1. On the *Compliance* tab, view the name of the user beside the *View Details* link.
2. Click the *View Details* link to view the following information:

Online/offline	Displays whether the endpoint is online or offline. A green icon indicates the endpoint is online.
Off-Net/On-Net	Displays whether the endpoint is on-net or off-net. A green *On-Net* icon indicates the endpoint is on-net. A gray *off-net* icon indicates the endpoint is off-net. See On-net / off-net status with FortiGate and EMS on page 59.
Username	Displays the name of the user logged into FortiClient on the endpoint.
Hostname	Displays the name of the endpoint where FortiClient is installed.
Domain	Displays the name of the domain to which the endpoint is connected, if applicable.
Phone Number	Displays the endpoint user's phone number if added by the endpoint user. See Retrieving user details from cloud applications on page 55 and Adding phone number and email address manually on page 57.
Email Address	Displays the endpoint user's email address if added by the endpoint user. See Retrieving user details from cloud applications on page 55 and Adding phone number and email address manually on page 57.
Windows Login / AD	FortiClient automatically attempts to retrieve a picture of the endpoint user from Windows or Active Directory (AD) to provide a visual representation of the endpoint user. If a picture is defined for Windows or AD to use, FortiClient retrieves the picture.
Cloud applications	Enables the endpoint user to provide information to FortiClient from an account for a cloud application, such as a Linkedin, Google, Salesforce, and so on. After the endpoint user logs into the account, FortiClient attempts to retrieve the following information when available: name, picture, phone number, and email address. See Retrieving user details from cloud applications on page 55.
Specify	Enables the endpoint user to specify a picture by taking a photo or selecting an image file. A user picture is sometimes called an avatar. See Specifying user picture manually on page 57.

3. Click the *X* to close the dialog box.

Retrieving user details from cloud applications

You can direct FortiClient to retrieve information about you from one of the following cloud applications, if you have an account:

- Linkedin account
- Google account
- Salesforce account

FortiClient attempts to retrieve the following information after you log in:

- Username
- Phone number
- Email address
- Picture

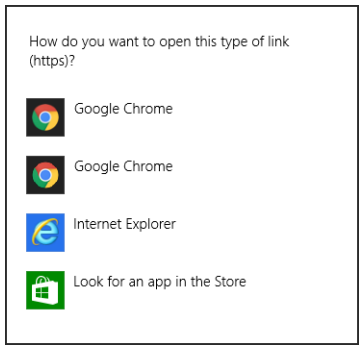
Although FortiClient can retrieve the endpoint user's username from cloud applications, the retrieved username does not display in FortiClient Console. Instead, the retrieved username is included in FortiClient logs with the phone number and email address. You can view log content in FortiOS, FortiAnalyzer, and FortiManager. See Sending logs to FortiAnalyzer or FortiManager on page 131.

You can manually specify a picture for FortiClient to use and edit the phone number and email address. See Specifying user picture manually on page 57 and Adding phone number and email address manually on page 57.

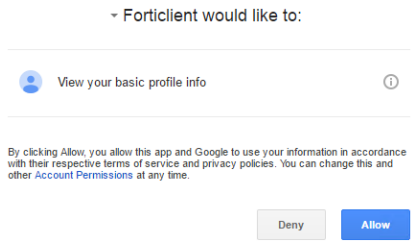
To retrieve user details from a cloud application:

1. On the *Compliance* tab, click the *View Details* link.
2. Click one of the following links:
   - *Linkedin Account*
   - *Google Account*
   - *Salesforce Account*

   The following window displays.



3. Click a browser and log into your account.
   The following page displays in the browser:



4. Click *Allow* to grant FortiClient permission to use your information.
5. Click *Save*.

Adding phone number and email address manually

Although FortiClient can retrieve information from a cloud application account, you can manually add or edit a phone number or email address in FortiClient Console.

The phone number can be a maximum of 30 characters and can include any of the following characters: *0123456789-+x*

To add a phone number and email address manually:

1. On the *Compliance* tab, click the *View Details* link.
2. Click the *Add Number* link, type a phone number and press Enter.
3. Click the *Add Email Address* link, type an email address and press Enter.

To edit a phone number or email address:

1. On the *Compliance* tab, click the *View Details* link.
2. Click the *Pencil* icon beside the phone number or email address, edit the information and press Enter.

Specifying user picture manually

Although FortiClient can retrieve a picture from Windows, Active Directory, or a cloud application, you can add a picture to FortiClient by taking a photo or uploading a picture.

To specify a user picture:

1. On the *Compliance* tab, click the *View Details* link.
2. Click the *Specify* link.
3. Perform one of the following actions:
   - Click *Take a picture* to take a picture. This option requires a web camera to be available on the endpoint.
   - Click *Browse* to select an image file.
4. Click *Save*.

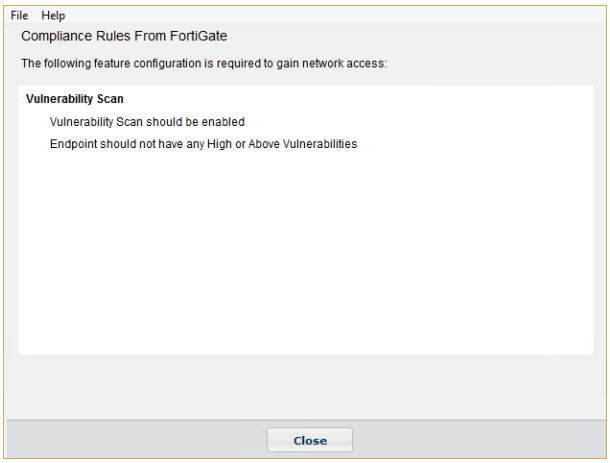
Viewing FortiGate compliance rules

When FortiClient Telemetry is connected to FortiGate, you can view the compliance rules from FortiGate. The compliance rules communicate the configuration required for FortiClient Console and the endpoint to remain compliant.

When the endpoint has a non-compliant status, an exclamation mark indicates which compliance rules are not met. See Viewing unmet compliance rules on page 62.

To view compliance rules:

1. On the *Compliance* tab, click the *Show Compliance Rules From <FortiGate>* link.
   The compliance rules from FortiGate display.



2. Click *Close* to return to the *Compliance* tab.

Viewing gateway IP lists

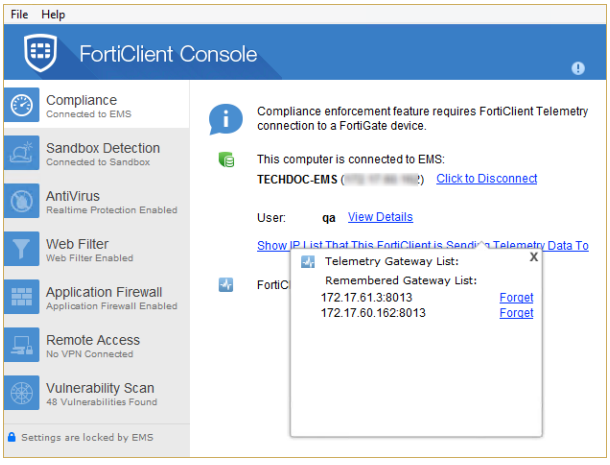
You can view the following gateway IP lists in FortiClient:

- Telemetry gateway list
  Administrators create the Telemetry gateway list. Endpoint users cannot change the list. See Telemetry gateway IP lists on page 26.
- Remembered FortiGate list
  Endpoint users create the Remembered FortiGate list. It is the list of remembered gateway IP addresses for FortiGate and EMS. When FortiClient Telemetry connects for the first time, you can instruct FortiClient to remember the gateway IP address for FortiGate or EMS. See Remembering gateway IP addresses on page 47.

The gateway IP lists are used to automatically connect FortiClient Telemetry to FortiGate or EMS.

To view gateway IP lists:

1. On the *Compliance* tab, click the *Show IP List That This FortiClient is Sending Telemetry Data to* link.
   The gateway IP list and the local gateway IP list display.



2. Click *X* to close the list.

Forgetting gateway IP addresses

When you instruct FortiClient to forget an IP address for FortiGate or EMS, FortiClient Telemetry does not use the IP address to automatically connect to FortiGate or EMS when rejoining the network.

To forget FortiGate or EMS:

1. On the *Compliance* tab, click *Show IP List That This FortiClient is Sending Telemetry Data to*.
2. In the *Remembered FortiGate List*, click *Forget* beside the gateway IP addresses you no longer want FortiClient to remember.
3. Click *X* to close the list.

On-net / off-net status with FortiGate and EMS

Endpoints must connect FortiClient Telemetry to FortiGate or EMS for FortiClient Console to display an on-net, off-net, or offline status.

The following rules identify when FortiGate, EMS, or FortiClient determine the status:

- When endpoints connect FortiClient Telemetry to FortiGate or EMS, FortiGate or EMS determines whether the endpoint has an on-net or off-net status.
- When endpoints cannot connect FortiClient Telemetry to FortiGate or EMS, FortiClient determines the on-net or off-net status, based on the on-net subnets.

When FortiGate and EMS are integrated, the primary FortiClient Telemetry connection is to FortiGate, and FortiGate calculates the status.

FortiGate

The version of FortiClient and FortiOS do not affect the on-net, off-net, or online status. The following examples show how FortiGate determines the status for the endpoint:

- The endpoint has a status of on-net when the endpoint is behind a FortiGate, and the endpoint receives option 224 with the FortiGate serial number. In this case, FortiGate is the DHCP server, and FortiGate checks that the serial number matches its own serial number.
- The endpoint has a status of on-net when the endpoint is inside one of the on-net subnets defined by FortiGate. You can configure on-net subnets in the FortiClient profile by using the FortiOS CLI and the `set on-net addr` command.
- The endpoint has a status of off-net when the endpoint is outside of the FortiGate network, such as connected through an external interface or hasn't received option 224 with the FortiGate serial number.
- The endpoint has a status of offline when the endpoint cannot connect FortiClient Telemetry to FortiGate and the endpoint is outside one of the on-net networks, even when option 224 and the FortiGate serial number are configured.
- The endpoint has a status of offline on-net when the endpoint is inside one of the on-net networks, but cannot connect FortiClient Telemetry to FortiGate.

For FortiClient to be in an on-net network, the IP address of FortiGate or EMS should be routed via the IP address from the on-net network.

EMS

The version of FortiClient and EMS do not affect the on-net, off-net, or online status. The following table shows how various configurations determine the status for the endpoint when FortiClient Telemetry is connected to EMS:

EMS DHCP on-net / off-net setting	On-net subnet	Option 224 serial number	Endpoint status
Off	No	N/A	On-net
On	No	Option not configured	Off-net
On	No	Option configured	On-net
Off or on	Yes and match	Configured or not	On-net
Off or on	Yes and do not match	Configured or not	Off-net

The following examples show how EMS determines the status for the endpoint:

- The endpoint has a status of offline when the endpoint cannot connect FortiClient Telemetry to EMS, and the endpoint is outside one of the on-net networks.
- The endpoint has a status of offline on-net when the endpoint cannot connect FortiClient Telemetry to EMS, but the endpoint is inside one of the on-net networks.

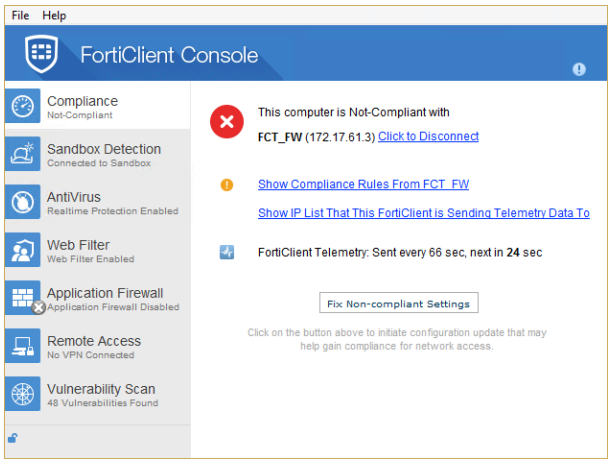
On-net subnets have higher priority over other settings. In addition, EMS doesn't compare the Option 224 serial number. As long as the endpoint has the serial number, EMS assumes that the endpoint is behind a FortiGate and is on-net.

Logging to FortiAnalyzer

When FortiClient endpoints are on-net, FortiClient logs are sent to FortiAnalyzer. However, when FortiClient endpoints are off-net, and FortiAnalyzer is not reachable, FortiClient logs are held for the log retention period, and sent to FortiAnalyzer when FortiClient is on-net again. By default, FortiClient logs are held for 90 days. You can control the log retention period by using the `<log_retention_days>` element in the XML configuration. See the *FortiClient XML Reference*.

Fixing not compliant (blocked)

When an endpoint is not compliant with FortiGate compliance rules, and FortiGate is configured with a non-compliance action of block, the endpoint is blocked from accessing the network, and the *Compliance* tab displays a not-compliant status:



The following information displays on the *Compliance* tab:

Compliance status	Indicates the endpoint is not compliant with FortiGate compliance rules and may be blocked from accessing the network. You have some time to fix the non-compliant issues before FortiGate blocks network access. See Compliance and vulnerability scanning on page 123.
Compliance rules	View the compliance rules by clicking the *Show Compliance Rules from <FortiGate>* link and see which rules are unmet.
IP list for FortiClient Telemetry	Click the *Show IP List That This FortiClient is Sending Telemetry Data To* link to view the gateway IP list being used for FortiClient Telemetry connection.
Fix non-compliance settings	Click the *Fix Non-Compliant Settings* button to try and return FortiClient to a compliant status. This option is not available when FortiClient settings are locked by EMS.

You can take the following steps to fix the not-compliant status and return the endpoint to a compliant status:

- View which compliance rules are unmet. See Viewing unmet compliance rules on page 62.
- Update the FortiClient configuration, if the option is available. See Fixing non-compliant settings on page 63.
- Fix detected vulnerabilities by using the automatic patching features. See Automatically fixing detected vulnerabilities on page 125.
- Manually install software patches, if required. See Manually fixing detected vulnerabilities on page 127.
- Manually fix system compliance:
- Create or modify the requested registry
- Create or modify the requested files or folders
- Start the requested processes

FortiClient must be installed with the correct setup to adhere to the compliance rules. See FortiClient setup types and modules on page 30.

Viewing unmet compliance rules

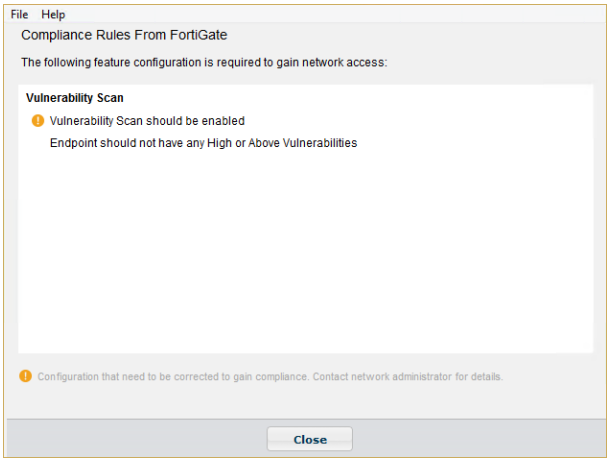
When an endpoint has a not-compliant (blocked) status, you can view the compliance rules from FortiGate and identify which ones are causing the not-compliant status.

To view not-compliant rules:

1. On the *Compliance* tab, click the *Show Compliance Rules From <FortiGate>* link.

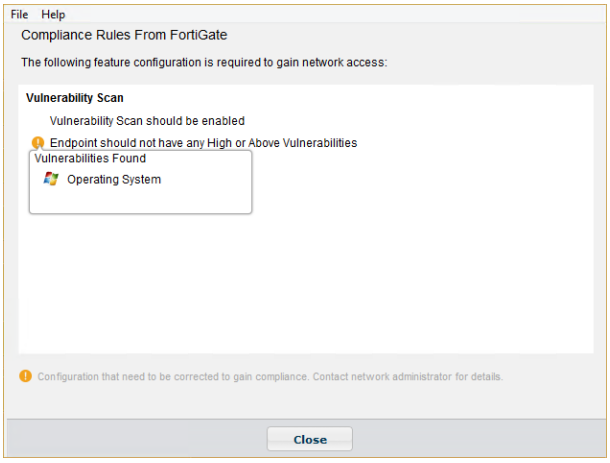
   The compliance rules from FortiGate display and the exclamation mark indicates an unmet compliance rule.

   In the following example, the compliance rule states that *Vulnerability Scan should be enabled*, and *Endpoint should not have any High or Above Vulnerabilities*. The exclamation mark indicates FortiClient or the endpoint is failing to meet the compliance rule.



2. Click the exclamation mark to view information about what is not compliant.

   A popup bubble message displays that identifies what part of the FortiClient configuration is not compliant. In this example, vulnerabilities were found for the Windows operating system.



3. Click *Close* to return to the *Compliance* tab.

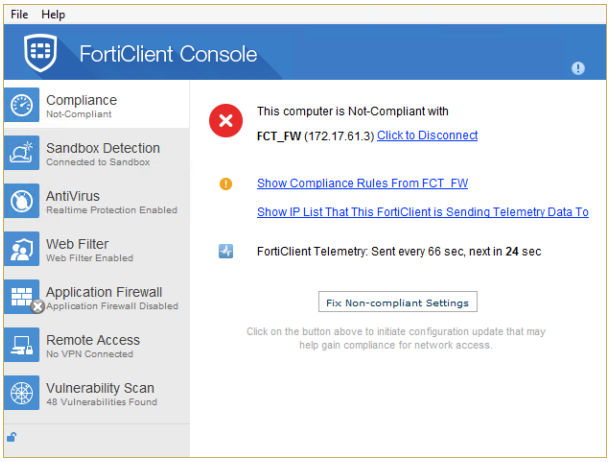
Fixing non-compliant settings

When the endpoint has a not-compliant status, and settings are unlocked, the *Fix Non-Compliant Settings* option displays on the *Compliance* tab. You can click the option to try and return FortiClient to a compliant state.

When FortiClient has a not-compliant status, and the *Fix Non-Compliant Settings* link does not display, endpoint users should contact their system administrator for help with configuring the endpoint and FortiClient Console to remain compliant with FortiGate.

To fix not-compliant settings:

1. On the *Compliance* tab, click *Fix Non-compliant Settings*.
   FortiClient attempts to return the endpoint to a compliant status by updating FortiClient settings to match the compliance rules from FortiGate, updating the FortiClient signatures, and patching detected vulnerabilities.



   The not-compliant settings are fixed, and the endpoint returns to a compliant status.

Patching software vulnerabilities

Endpoints can become not-compliant when vulnerabilities are detected for software that is installed on the endpoint, but software patches for the vulnerabilities are not yet installed. The vulnerabilities must be patched for FortiClient to return to a compliant status. See Automatically fixing detected vulnerabilities on page 125 and Manually fixing detected vulnerabilities on page 127.

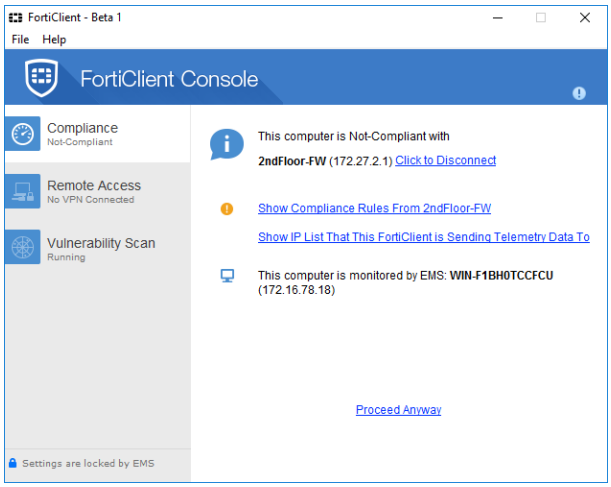
Examples of blocked network access

The following table provides examples of when endpoints are blocked from accessing the network and how you can regain access.

Symptom	Cause of blocked access	Solution
No network access and no FortiClient software installed	FortiClient is not installed and FortiClient Telemetry is not connected.	FortiGate displays a portal in a web browser and the portal includes a link to the FortiClient installer. Download and install FortiClient software and connect FortiClient Telemetry to FortiGate. See Connecting FortiClient Telemetry after installation on page 46
No network access and a *Not Participating* status on the *Compliance* tab in FortiClient Console	FortiClient Telemetry is not connected	In FortiClient console, connect FortiClient Telemetry to FortiGate. See Connecting FortiClient Telemetry manually on page 49.
No network access and *Not Compliant* status on the *Compliance* tab in FortiClient Console	Endpoint software or FortiClient configuration does not meet compliance rules.	View unmet compliance rules and configure FortiClient to meet them. In some cases, you may need to contact your system administrator for help. See Viewing unmet compliance rules on page 62.
	The *Vulnerability Scan* tab shows detected vulnerabilities	Fix detected vulnerabilities. See Automatically fixing detected vulnerabilities on page 125. You may also need to manually fix detected vulnerabilities. See Manually fixing detected vulnerabilities on page 127.
No network access and *Compliant* status on the *Compliance* tab in FortiClient Console	FortiGate is configured to warn endpoint users about network access and you have not clicked the *I Agree* button.	Click the *I Agree* button in the web portal browser displayed by FortiGate. See Fixing not compliant (warning) on page 64.

Fixing not compliant (warning)

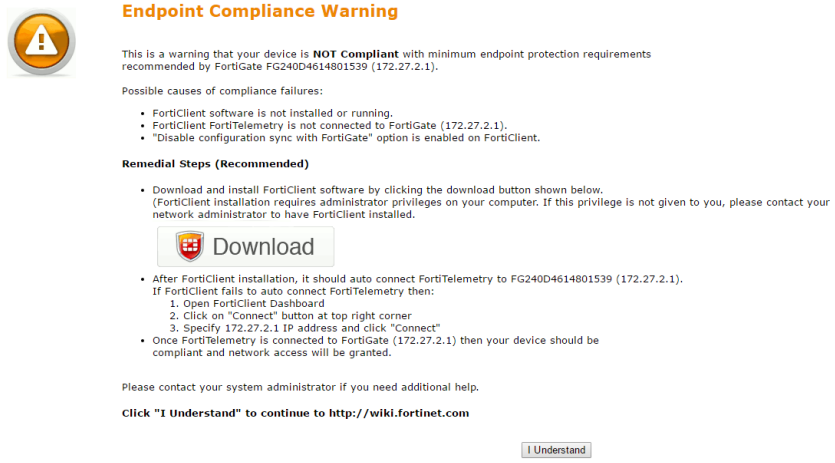
When an endpoint is not compliant with FortiGate compliance rules, and FortiGate is configured with a non-compliance action of to warn, the *Compliance* tab displays the following information icon with not-compliant status:



The following information displays on the *Compliance* tab:

Compliance status	Indicates the endpoint is warned about the not-compliant status with FortiGate compliance rules. Access to the network is blocked until the endpoint user acknowledges the warning by clicking the *Proceed Anyway* button in FortiClient Console or the *I Agree* button in the FortiGate web portal.
Compliance rules	View the compliance rules by clicking *Show Compliance Rules from <FortiGate>* and see which compliance rules are unmet.
IP list for FortiClient Telemetry	Click *Show IP List That This FortiClient is Sending Telemetry Data To* to view the gateway IP list used for FortiClient Telemetry connection.
Fix Non-Compliant Settings	Click the *Fix Non-Compliant Settings* button to try and return FortiClient to a compliant status. This option is not available when EMS has locked FortiClient settings.
Proceed Anyway	Click *Proceed Anyway* to acknowledge the not-compliant status and access the network without fixing all reported issues.

FortiGate also displays a warning portal that includes an *I Agree* button at the bottom of the page:



When FortiGate warns endpoints about a not-compliant status, you can choose one of the following actions:

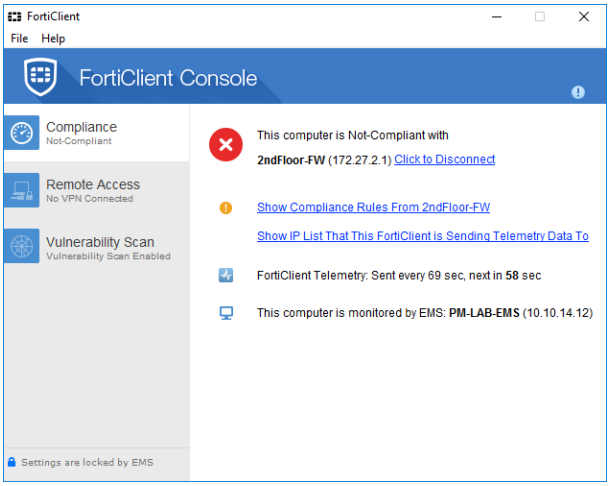
- Fix the not-compliant issues and return the endpoint to a compliant status, then access the network with a compliant status.
- Acknowledge the not-compliant status and access the network by clicking *Proceed Anyway* in FortiClient Console or *I Understand* in the warning portal.

If you choose to access the network without fixing the not-compliant issues, you must acknowledge the warning before you can access the network.

You only need to click *Proceed Anyway* in the FortiClient Console or *I Understand* in the warning portal. You do not need to click both buttons. After you click one button, the software communicate with each other to relay the acknowledgment. For example, if you click *Proceed Anyway* in the FortiClient Console, FortiClient communicates the acknowledgment to FortiGate, and you are not required to click *I Understand* in the warning portal.

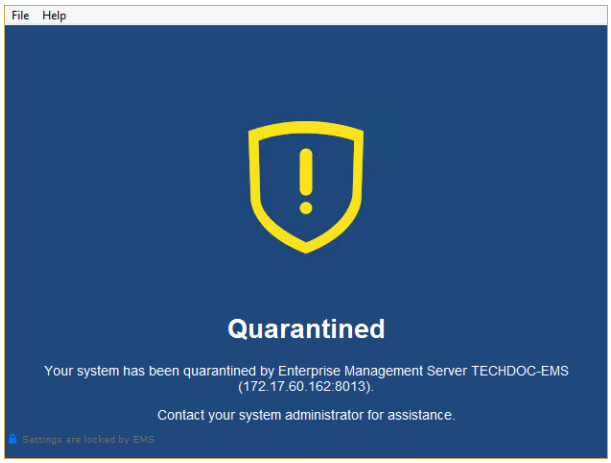
To proceed anyway:

1. On the *Compliance* tab, click *Proceed Anyway*.
   The not-compliant issues remain unfixed, but you are granted network access. Because the not-compliant issue remains unfixed, the icon changes to *Not-Compliant*.



Quarantined endpoints

In certain situations, an administrator may quarantine an endpoint. When an endpoint is quarantined, the following page displays, and the endpoint user loses network access. Contact your system administrator for assistance.


File Help
Quarantined
Your system has been quarantined by Enterprise Management Server TECHDOC-EMS (172.17.60.162:8013).
Contact your system administrator for assistance.
Settings are locked by EMS

Sandbox Detection

FortiClient supports integration with FortiSandbox. When configured, FortiSandbox automatically scans files executed on the endpoint or from removable media attached to the endpoint or mapped network drives. FortiSandbox can also automatically scan files downloaded from the Internet or emailed to the endpoint. Endpoint users can also manually submit files to FortiSandbox for scanning.

Access to files can be blocked until the FortiSandbox scanning result is returned.

When scanning is complete, FortiSandbox can quarantine infected files or alert and notify the endpoint user of infected files without quarantining the files.

As FortiSandbox receives files for scanning from various sources, it collects and generates AV signatures for such samples. FortiClient periodically downloads the latest AV signatures from FortiSandbox, and applies them locally to all realtime and on-demand AntiVirus scanning.

Enabling Sandbox Detection

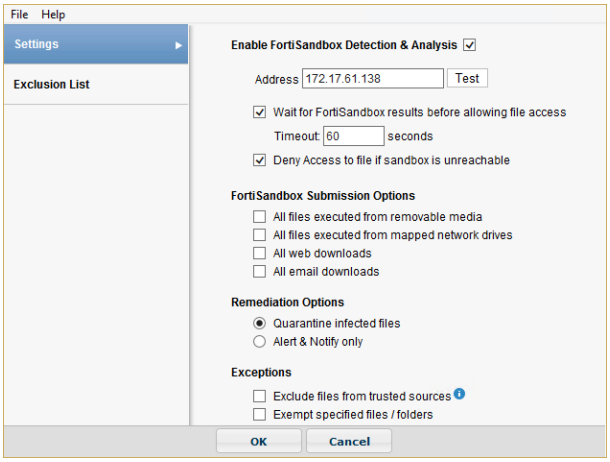
The *Sandbox Detection* tab displays in FortiClient Console when FortiClient is installed with *Advanced Persistent Threat (APT) Components* selected.

If you have a FortiSandbox unit, you can enable FortiClient to work with FortiSandbox.

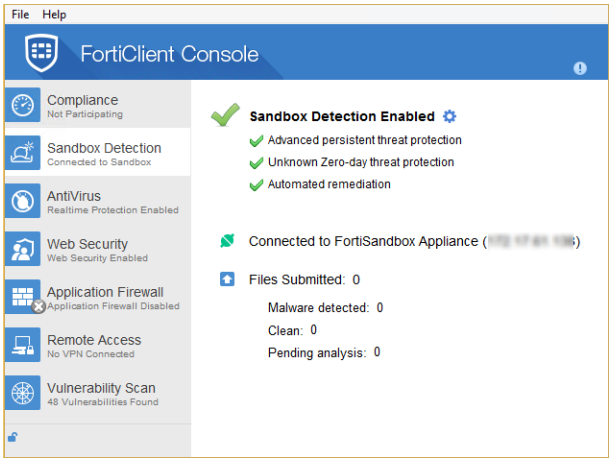
To enable Sandbox Detection:

1. On the *Sandbox Detection* tab, click the settings icon.
2. If the *Administrative privileges are required to change settings. Press Elevate to obtain these privileges.* message displays, click *Elevate*.

   The settings page displays.



3. Select the *Enable FortiSandbox Detection & Analysis* checkbox.
4. In the *Address* box, type the IP address for FortiSandbox, and click *Test* to ensure the IP address is valid.
   If the IP address is valid, a confirmation dialog box displays.
5. Click *OK* to close the confirmation dialog box.
6. Click *OK* to save the changes.
   For information about configuring FortiSandbox, see Configuring Sandbox Detection on page 71.
   FortiSandbox Detection is enabled.



Checking FortiClient authorization for FortiSandbox scanning

This feature requires FortiSandbox 2.5.0 or later. If you are using EMS, EMS 1.2.2 or later is required.

Depending on the FortiSandbox configuration, FortiSandbox may only scan submitted files when FortiClient is authorized. The *Sandbox Detection* tab in FortiClient Console displays the authorization status.

The following table summarizes how FortiSandbox receives the authorization status for FortiClient:

Mode	FortiClient Telemetry connection	FortiClient authorization
Standalone mode	N/A	The FortiSandbox administrator can choose to disable authorization of FortiClient. When authorization is disabled, all authorization requests are accepted. When authorization is enabled, the FortiSandbox administrator must manually authorize each FortiClient using the FortiSandbox GUI.

Mode	FortiClient Telemetry connection	FortiClient authorization
Managed mode	EMS only	EMS provides authorization to FortiSandbox for FortiClient. The FortiSandbox administrator must authorize the EMS server managing FortiClient.
	EMS and FortiGate	EMS provides authorization to FortiSandbox for FortiClient. The FortiSandbox administrator can authorize EMS or FortiGate.
	FortiGate only	FortiGate provides authorization to FortiSandbox for FortiClient. The FortiSandbox administrator must authorize FortiGate.

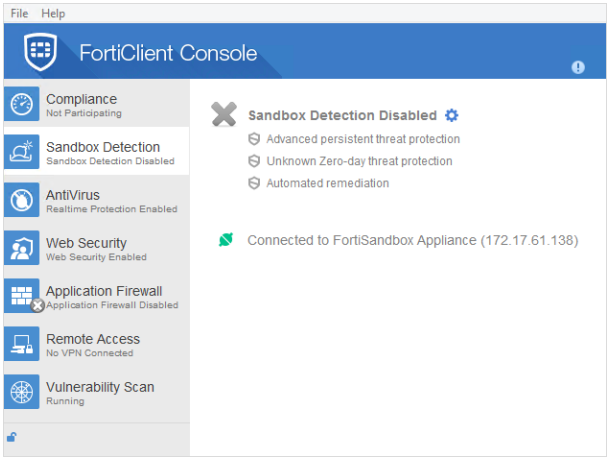
To check Sandbox authorization status:

1. On the *Sandbox Detection* tab, click the settings icon.
2. If the *Administrative privileges are required to change settings. Press Elevate to obtain these privileges.* message displays, click *Elevate*.
   The settings page displays.
3. Under *Enable FortiSandbox Detection & Analysis*, click the *Test* button.
   A dialog box communicating the authorization status displays.
4. Click *OK* to close the confirmation dialog box.

Disabling Sandbox Detection

To disable Sandbox Detection:

1. On the *Sandbox Detection* tab, click the settings icon.
   The settings page displays.
2. Clear the *Enable FortiSandbox Detection & Analysis* checkbox, and click *OK*.
   FortiSandbox Detection is disabled.



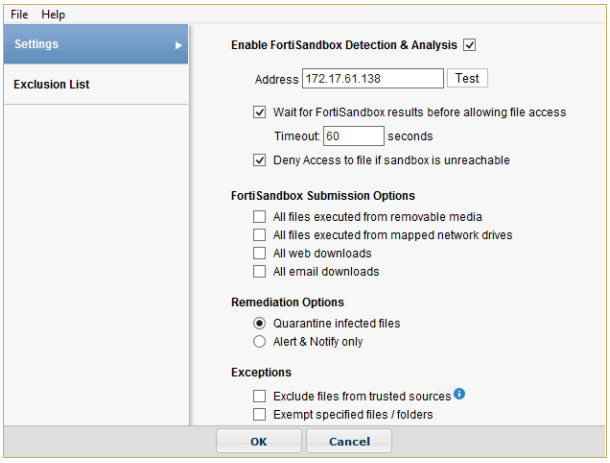
Configuring Sandbox Detection

You can configure what files are automatically submitted from the endpoint to FortiSandbox for scanning. You can also configure whether FortiSandbox quarantines infected files and whether to exclude any files or folders from FortiSandbox scanning.

Configuring submission, access, and remediation

To configure submission, access, and remediation:

1. On the *Sandbox Detection* tab, click the *Settings* icon.
   The settings page displays.



2. Set the following options, and click *OK*:

	Wait for FortiSandbox results before allowing file access	Select to wait for FortiSandbox analysis results before files can be accessed. Clear the checkbox to allow file access before FortiSandbox results are known.
	Timeout seconds	Specify the timeout duration in seconds. After the time expires, file access is allowed, even if FortiSandbox has not returned results and if the *Deny Access to file if Sandbox unreachable* option is disabled. When set to *0*, the downloaded file is always released and the popup never displays. See Using the popup window on page 78.
	Deny Access to file if Sandbox is unreachable	Select to deny access to files when FortiClient cannot reach FortiSandbox for file analysis. Clear the checkbox to allow file access if the FortiSandbox unit cannot be reached for scanning. See Examples of FortiSandbox availability and scanning results on page 72.
FortiSandbox Submission Options		

	All files executed from removable media	Select to submit all files executed on removable media, such as USB drives, to FortiSandbox for analysis. Clear the checkbox to disable this feature.
	All files executed from mapped network drives	Select to submit all files that are executed on mapped network drives to FortiSandbox for analysis. Clear the checkbox to disable this feature.
	All web downloads	Select to submit all web downloads on the endpoint to FortiSandbox for analysis. Clear the checkbox to disable this feature.
	All email downloads	Select to submit all email downloads on the endpoint to FortiSandbox for analysis. Clear the checkbox to disable this feature.
Remediation Options		
	Quarantine infected files	Select to quarantine infected files.
	Alert & Notify only	Select to alert and notify the endpoint user about infected files, but not quarantine infected files.

Examples of FortiSandbox availability and scanning results

The following table identifies how the FortiSandbox settings and availability affect file scanning results when the Sandbox `<timeout>` setting is not zero.

Deny access to file if unreachable	FortiSandbox reachable?	FortiSandbox timed out?	FortiSandbox final action	FortiSandbox message
Disabled	Yes	No	Based on FortiSandbox verdict	Scanning verdict is displayed
Disabled	Yes	Yes	Release file	Scanning timed out
Disabled	No	N/A	Release file	Scanning skipped - FortiSandbox unreachable
Enabled	Yes	No	Based on FortiSandbox verdict	Scanning verdict is displayed
Enabled	Yes	Yes	Block file	Scanning timed out - access denied
Enabled	No	N/A	Block file	Scanning skipped - FortiSandbox unreachable - access denied

Configuring exceptions

To configure exceptions:

1. On the *Sandbox Detection* tab, click the *Settings* icon.
   The settings page displays.
2. Set the following options and click *OK*:

Exceptions		
	Exclude files from trusted sources	Select to exclude files from trusted sources from FortiSandbox analysis. Click the *i* icon to view the list of trusted sources. You cannot change the list of trusted sources.
	Exempt specified files / folders	Select to exempt specified files and/or folders from FortiSandbox analysis. You must also create the exclusion list.

3. If you selected the *Exempt specified files /folders*, you must create the exclusion list. See Managing the Sandbox Detection exclusion list on page 73.

Managing the Sandbox Detection exclusion list

You can add files and folders to the exclusion list for FortiSandbox. FortiSandbox does not scan the identified files or folders when the *Exempt specified files / folders* checkbox is selected. See Configuring exceptions on page 73.

You can also remove files and folders from the exclusion list.

To add files or folders to the exclusion list:

1. On the *Sandbox Detection* tab, click the *Settings* icon.
   The Settings page displays.
2. Click the *Exclusion List* tab.
   The exclusion list displays.
3. Click the + icon, and select *Add file* or *Add folder*.
   A Browse dialog box displays.
4. Locate and select the file or folder, and click *Open*.
   The file or folder is added to the exclusion list, and will not be scanned by FortiSandbox.
5. Click *OK* to save the changes.

To remove files or folders from the exclusion list:

1. On the *Sandbox Detection* tab, click the *Settings* icon.
   The Settings page displays.
2. Click the *Exclusion List* tab.
   The exclusion list displays.
3. Click one or more items in the exclusion list.
   A checkmark displays beside the selected items.

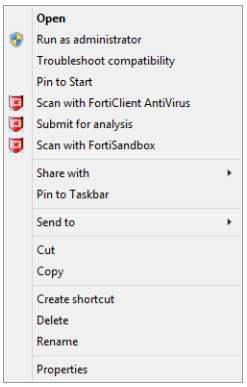
4. Click the - icon.
   The selected items are removed from the exclusion list.
5. Click *OK* to save the changes.

Scanning with FortiSandbox on demand

You can send files to FortiSandbox for scanning on demand when FortiSandbox is enabled and online.

To scan with FortiSandbox on demand:

1. Right-click a file and select *Scan with FortiSandbox* from the menu.



Viewing Sandbox Detection results

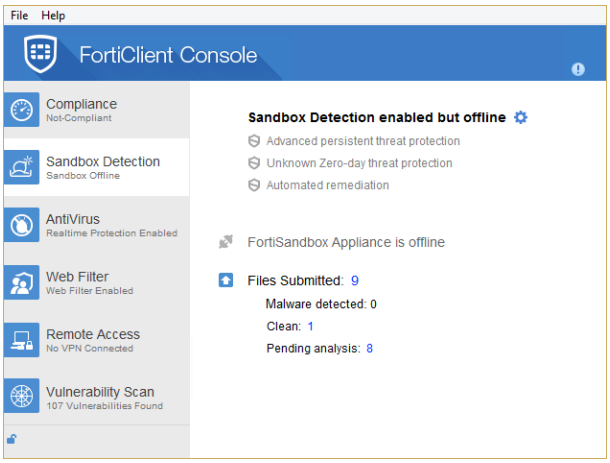
FortiSandbox scan results display on the *Sandbox Detection* tab and in a popup.

When a virus is detected, FortiClient creates a notification alert. See Viewing notifications on page 79.

Viewing FortiSandbox scan results

To view FortiSandbox scan results:

1. Go to the *Sandbox Detection* tab.



The following information displays:

Files Submitted	Displays the number of files submitted to FortiSandbox for scanning.
Malware detected	Displays the number of detected malware files. Click the *<number>* link beside *Malware detected* to view details about the files.
Clean	Displays the number of files determined clean after FortiSandbox scanning.
Pending analysis	Displays the number of files waiting for FortiSandbox scanning.

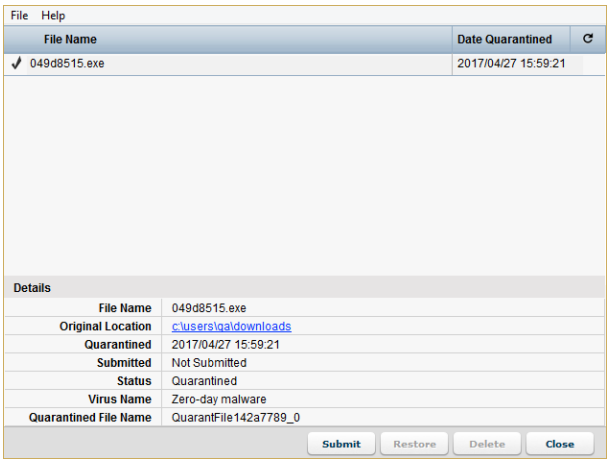
Viewing quarantined files

You can view files quarantined by FortiSandbox. You can also restore and delete quarantined files and submit quarantined files for analysis again.

You cannot restore and delete quarantined files when FortiClient is in managed mode.

To view quarantined files:

1. Go to the *Sandbox Detection* tab.
2. Beside *Malware detected*, click the *<number>* link to view quarantined files.
   The list of files displays.



The following information displays:

Summary		
	File Name	Lists the names of the quarantined files.
	Date Quarantined	Lists the date and time FortiSandbox quarantined the files.
	Refresh	Click to refresh the information.
Details		Select a file from the list to view detailed information.
	File Name	Name of the selected quarantined file.
	Original Location	Location of the file before FortiSandbox scanning.
	Quarantined	Date and time FortiSandbox quarantined the file.
	Submitted	Displays *Not Submitted* when the selected file has not been submitted to FortiGuard for analysis by clicking the *Submit* button. Displays *Submitted* after clicking the *Submit* button.
	Status	Status of the file, such as *Quarantined*.
	Virus Name	Name of the virus FortiSandbox detected.
	Quarantined File Name	Name of the file after it was quarantined.
Submit		Click submit for FortiGuard analysis.
Restore		Click to remove the selected file from quarantine.
Delete		Click to delete the selected file from the device.

3. Select a file from the list to view detailed information about the file.
4. Click *Close*.

Submitting quarantined files for scanning

You can submit quarantined files to FortiSandbox for scanning.

To submit quarantined files for scanning:

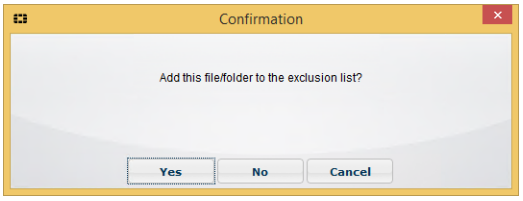
1. Go to the *Sandbox Detection* tab.
2. Beside *Zero-day malware*, click the *<number>* link to view quarantined files.
   The list of files displays.
3. Select the file and click *Submit*.

Restoring quarantined files

Endpoint users can only restore quarantined files with FortiClient in standalone mode. When you restore a quarantined file, you can choose whether to add the file to the exclusion list.

To restore quarantined files:

1. Go to the *Sandbox Detection* tab.
2. Beside *Zero-day malware*, click the *<number>* link to view quarantined files.
   The list of files displays.
3. Select the file and click *Restore*.
   A confirmation dialog box displays.



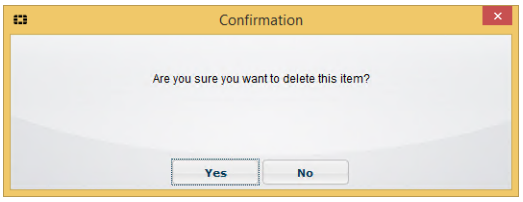
4. Click *Yes* to restore the file and add it to the exclusion list or *No* to restore the file without adding it to the exclusion list.
5. If the *Administrative privileges are required to change settings. Press Elevate to obtain these privileges.* message displays, click *Elevate*.
   The file is restored.

Deleting quarantined files

Endpoint users can only restore quarantined files with FortiClient in standalone mode.

To delete quarantined files:

1. Go to the *Sandbox Detection* tab.
2. Beside *Zero-day malware*, click the *<number>* link to view quarantined files.
   The list of files displays.
3. Select the file, and click *Delete*.
   A confirmation dialog box displays.

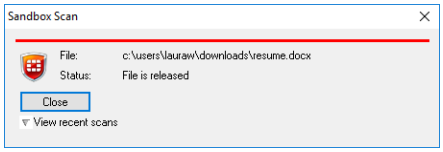


4. Click *Yes*.
   The file is deleted.

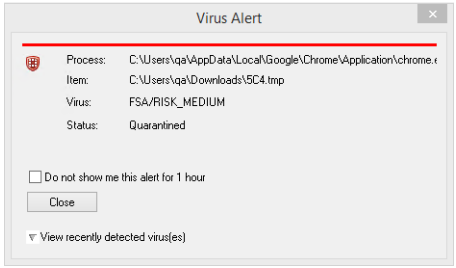
Using the popup window

The settings for the *Wait for FortiSandbox scan result before allowing file access* and *Timeout seconds* options affect when the popup displays. See Configuring Sandbox Detection on page 71.

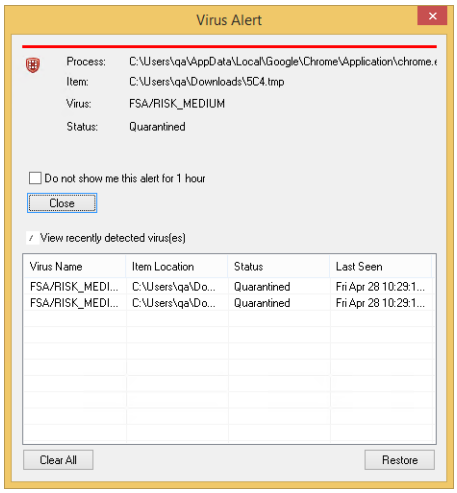
As FortiSandbox scans and releases files, a popup displays to inform you. You can view the recent scans by clicking the *View recent scans* option.



When FortiSandbox detects a virus and quarantines a file, the *Virus Alert* window displays.



You can use the *Virus Alert* window to view information about the recently scanned files by clicking the *View recently detected virus(es)* option.



With the information expanded, you can select a quarantined file and click the *Restore* button to restore the file.

Endpoint users can only restore quarantined files with FortiClient in standalone mode.

Viewing notifications

Click the notifications icon in FortiClient Console to view notifications. When a virus has been detected, the notifications icon changes from gray to yellow or red.

Event notifications include:

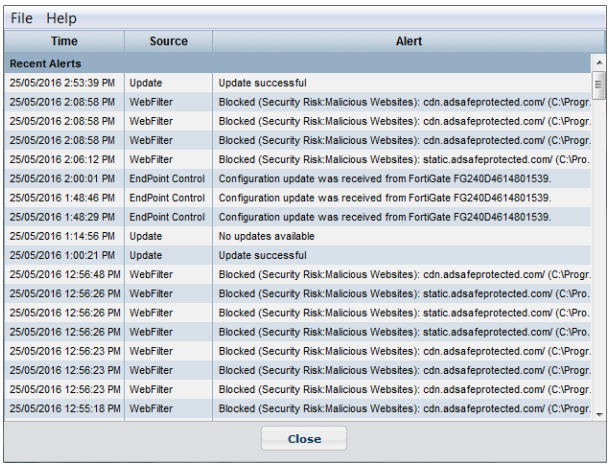
- Sandbox Detection events, including detected malware
- Antivirus events, including scheduled scans and detected malware.
- Endpoint Control events, including configuration updates received from FortiGate or EMS.
- Web Filter events, including blocked web site access attempts.
- System events, including signature and engine updates and software upgrades.

Click *Threat Detected* to view quarantined files, site violations, and realtime protection events.

For FortiClient in standalone mode, you can clear the entries by clicking the *Clear* button. This option is not available for FortiClient in managed mode.

To view notifications:

1. In FortiClient Console, click the *Notifications* icon (an exclamation mark) in the top-right corner.
   The list of notifications displays.



2. Click *Close* to close the list.

Antivirus

FortiClient includes an antivirus component to scan system files, executable files, removable media, dynamic-link library (DLL) files, and drivers. FortiClient also scans for and removes rootkits. In FortiClient, file-based malware, malicious websites, phishing, and spam URL protection are part of the antivirus component.

FortiClient also includes an anti-exploit detection feature that helps protect endpoints from unknown exploit attacks.

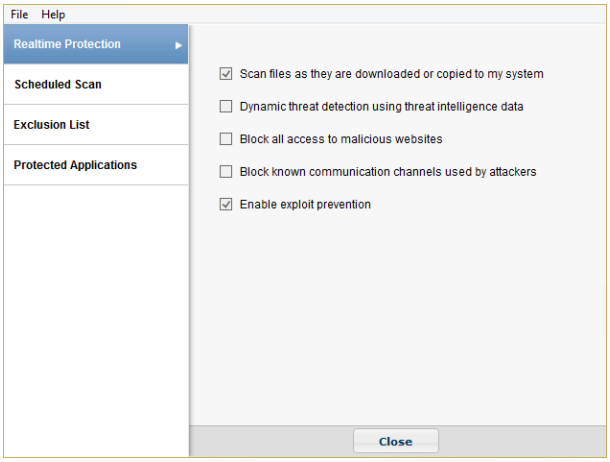
Enabling realtime protection

The *AntiVirus* tab displays in FortiClient Console when FortiClient is installed with *Additional Security Features* and *AntiVirus* selected.

For FortiClient in managed mode, when FortiClient Telemetry is connected to FortiGate or EMS, an administrator may enable, configure, and lock realtime protection. You can enable realtime protection if EMS has not locked FortiClient Console and realtime protection is excluded from FortiGate compliance rules.

To enable realtime protection:

1. On the *AntiVirus* tab, click the *Settings* icon.
   The realtime protection settings page opens.
2. Select the *Scan files as they are downloaded or copied to my system* checkbox.



3. (Optional) Set the following options:

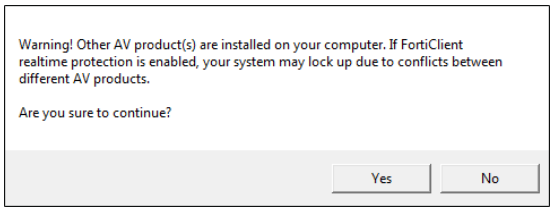
Dynamic threat detection using threat intelligence data	Select to use threat intelligence data to provide dynamic threat detection. The *Scan files as they are downloaded or copied to my system* checkbox must be selected to enable dynamic threat detection. Clear to disable dynamic threat detection.
Block all access to malicious websites	Select to block all access to malicious websites. Clear to allow access to malicious websites. See Blocking access and communication channels on page 83.
Block known communication channels used by attackers	Select to block known communication channels uses by attackers. Clear to allow access to known communication channels used by attackers. See Blocking access and communication channels on page 83.
Enable exploit prevention	Select to protect applications from exploits. Clear to disable exploit prevention. See Enabling and disabling exploit prevention on page 94.

4. Click *OK*.

If your system has another antivirus program installed, FortiClient displays a warning that your system may lock up due to conflicts between different antivirus products. See Third party antivirus software and realtime protection on page 82.

Third party antivirus software and realtime protection

For FortiClient in standalone mode, it is recommended to remove third party antivirus products before installing FortiClient or enabling the antivirus realtime protection feature. Otherwise you may see the following conflicting antivirus warning when you enable realtime protection:



In managed mode, when FortiClient Telemetry is connected to FortiGate, the FortiGate compliance rules may allow third party antivirus software to be used as part of the compliance rules. In this case, you should disable realtime protection in FortiClient Console.

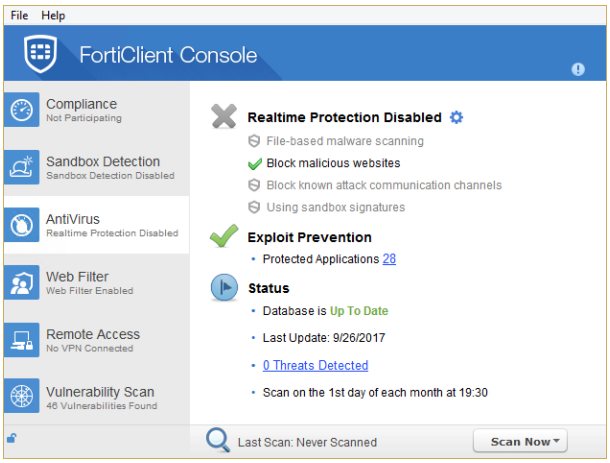
Disabling realtime protection

When FortiClient Telemetry is connected to FortiGate or EMS, you may be unable to disable realtime protection. You can disable realtime protection when EMS has not locked FortiClient Console and realtime protection is excluded from FortiGate compliance rules.

You can disable realtime protection but leave the following options enabled: *Block all access to malicious websites* and *Block known communication channels used by attackers*. You cannot disable exploit prevention.

To disable realtime protection:

1. On the *AntiVirus* tab, click the *Settings* icon.
   The realtime protection settings page opens.
2. Clear the *Scan files as they are downloaded or copied to my system* checkbox and click *OK*.



Configuring AntiVirus

You can block access and communication channels, update the antivirus database, schedule antivirus scanning, add files or folders to exclusion lists, and configure additional antivirus options.

Blocking access and communication channels

The Web Security/Web Filter module must be installed before you can enable these features.

To block access and communication channels:

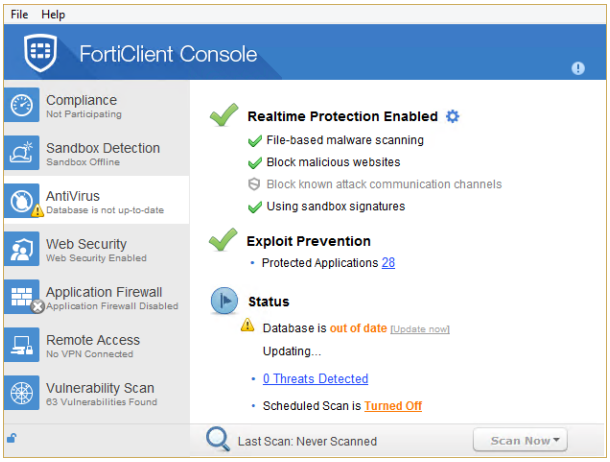
1. On the *AntiVirus* tab, select the settings icon to open the realtime protection settings page.
2. Select the *Block all access to malicious websites* checkbox.
3. Perform one of the following actions:
   - Select the *Use Web Filter exclusion list* checkbox if you want to use the exclusion list for the *Web Security/Web Filter* tab. See Managing the Web Filter/Web Security exclusion list on page 101.
   - Clear the *Use Web Filter exclusion list* checkbox to use the exclusion list for the *Antivirus* tab. You must define an exclusion list. See Managing the AntiVirus exclusion list on page 85.
4. Select the *Block known communication channels used by attackers* checkbox.
5. Click *OK*.

Updating Antivirus database

FortiClient informs you if the AntiVirus database is out of date. FortiClient automatically updates signatures. However, if you see the signatures are outdated, you can click *Update now*. See Viewing FortiClient engine and signature versions on page 93.

To update the AntiVirus database:

1. On the *AntiVirus* tab, click *Update Now*.



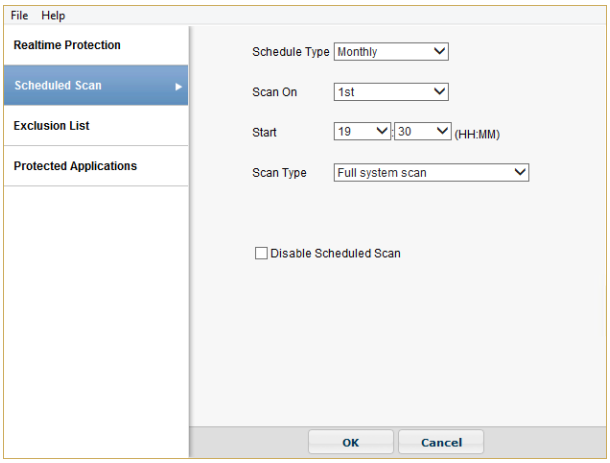
The AntiVirus database is updated.

Scheduling antivirus scanning

If you configure monthly scans to occur on the 31st of each month, the scan occurs on the first day of the month for months with fewer than 31 days.

To schedule antivirus scanning:

1. On the *AntiVirus* tab, click the *Settings* icon beside *Realtime Protection*.
2. Click the *Scheduled Scan* tab.



3. Configure the following settings:

Schedule Type	Select *Daily*, *Weekly*, or *Monthly* from the dropdown list.
Scan On	For weekly scheduled scans, select the day of the week in the dropdown list. For monthly scheduled scans, select the day of the month in the dropdown list.
Start	Select the time of day to start the scan. The time format uses a 24-hour clock.
Scan Type	Select the scan type: • *Quick system scan* runs the rootkit detection engine to detect and remove rootkits. It only scans the following items for threats: executable files, DLLs, and drivers that are currently running. • *Full system scan* runs the rootkit detection engine to detect and remove rootkits. It then performs a full system scan of all files, executable files, DLLs, and drivers. • *Custom scan* runs the rootkit detection engine to detect and remove rootkits. It allows you to select a specific file folder on your local hard disk drive (HDD) to scan for threats. You cannot schedule a removable media scan. A full scan scans removable media.
Disable Scheduled Scan	Select to disable scheduled scan.

4. Click *OK* to save the setting and return to the main FortiClient Console.

Managing the AntiVirus exclusion list

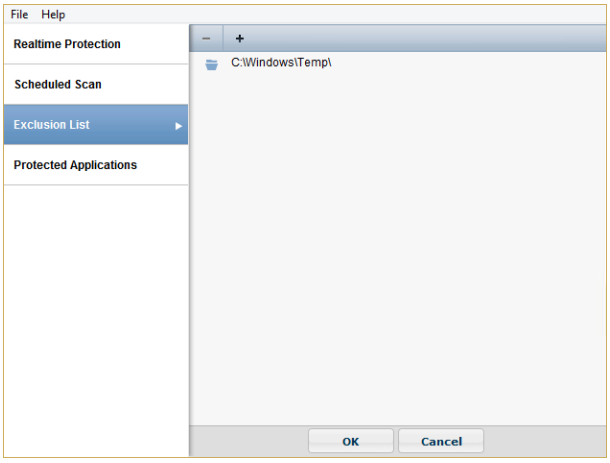
FortiClient supports using wildcards and path variables to specify files and folders to exclude from scanning. The following wildcards and variables are supported, among others:

- Using wildcards to exclude a range of file names with a specified extension, such as Edb*.jrs
- Using wildcards to exclude all files with a specified extension, such as *.jrs
- Path variable %windir%
- Path variable %allusersprofile%
- Path variable %systemroot%
- Path variable %systemdrive%

Combinations of wildcards and variables are not supported.

To add files or folders to the AntiVirus exclusion list:

1. On the *AntiVirus* tab, click the *Settings* icon.
2. Click the *Exclusion List* tab.
3. Click the + icon, and select *Add file* or *Add folder*.



A Browse dialog box displays.

4. Locate and select the file or folder, and click *Open*.
   The file or folder is added to the exclusion list, and will not be scanned by the AntiVirus engine.
5. Click *OK* to save the changes.

To remove files or folders from the AntiVirus exclusion list:

1. On the *AntiVirus* tab, click the *Settings* icon.
   The Settings page displays.
2. Click the *Exclusion List* tab.
   The exclusion list displays.
3. Click one or more items in the exclusion list.
   A checkmark displays beside the selected items.
4. Click the - icon.
   The selected items are removed from the exclusion list.
5. Click *OK* to save the changes.

Configuring additional Antivirus options

You can configure additional settings for the *Antivirus* tab by going to *File* > *Settings* in FortiClient Console. See Antivirus options on page 133.

Scanning with AntiVirus on demand

You can perform on-demand antivirus scanning. You can scan specific files or folders, and you can submit a file for analysis.

Scanning now

To perform on-demand antivirus scanning:

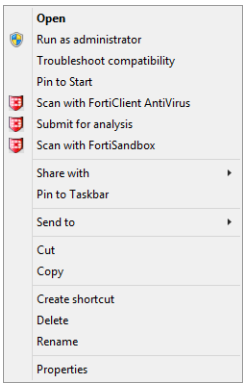
1. On the *AntiVirus* tab, click the *Scan Now* button.
2. Use the dropdown list to select *Custom Scan*, *Full Scan*, *Quick Scan*, or *Removable media Scan*.

Custom Scan	Runs the rootkit detection engine to detect and remove rootkits. It allows you to select a specific file folder on your local hard disk drive (HDD) to scan for threats.
Full Scan	Runs the rootkit detection engine to detect and remove rootkits. It then looks for threats by performing a full system scan on all files, executable files, DLLs, and drivers.
Quick Scan	Runs the rootkit detection engine to detect and remove rootkits. It looks for threats by scanning executable files, DLLs, and drivers that are currently running.
Removable Media Scan	Runs the rootkit detection engine to detect and remove rootkits. It scans all connected removable media, such as USB drives.

Scanning files or folders

To scan files or folders:

1. Right-click the file or folder and select *Scan with FortiClient AntiVirus* from the menu.



Submitting files to FortiGuard for analysis

You can send up to five files a day to FortiGuard for analysis.

You do not receive feedback for files submitted for analysis. The FortiGuard team can create signatures for any files submitted for analysis and determined to be malicious.

To submit files for analysis:

1. On your workstation, right-click a file or executable, and select *Submit for analysis* from the menu.
   A dialog box displays that identifies the number of files submitted.
2. Confirm the location of the file that you want to submit, and click the *Submit* button.

Viewing AntiVirus scan results

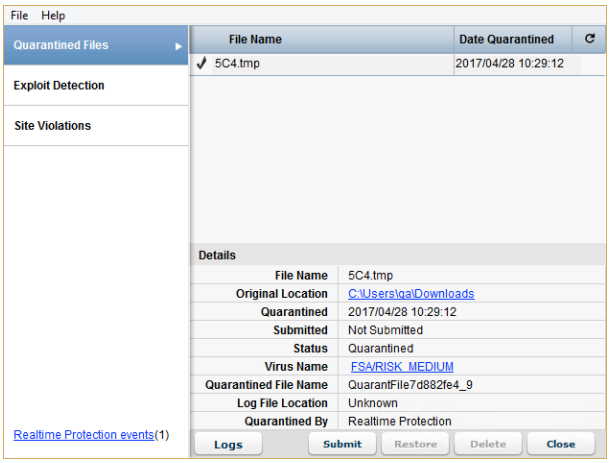
You can view quarantined threats, site violations, alerts, and realtime protection events when FortiClient is in standalone or managed mode.

Viewing quarantined threats

To view quarantined threats:

1. On the *AntiVirus* tab, click *X Threats Detected*.
2. Click the *Quarantined Files* tab.

   In this page you can view, restore, or delete the quarantined file. You can also view the original file location, virus name, and logs, and submit the suspicious file to FortiGuard.



This page displays the following information:

Summary		
	File Name	Lists the quarantined files' names.
	Date Quarantined	Lists the date and time FortiClient quarantined the files.
	Refresh	Click to refresh the information.
Details		Select a file from the list to view detailed information.
	File Name	Selected quarantined file's name.
	Original Location	File location before antivirus scanning.
	Quarantined	Date and time the file was quarantined.
	Submitted	Displays *Not Submitted* when the selected file has not been submitted to antivirus software for scanning by clicking the *Submit* button. Displays *Submitted* after clicking the *Submit* button.
	Status	Status of the file, such as *Quarantined*.
	Virus Name	Virus name as detected by antivirus software.
	Quarantined File Name	File name after it was quarantined.

	Log File Location	Log data location, if known.
	Quarantined By	Click to refresh the list.
	Submit	Click to submit the quarantined file to FortiGuard. Press and hold the Ctrl key to submit multiple entries.
Logs		Click to view the log files for antivirus scanning.
Submit		Click to submit the quarantined file for scanning.
Restore		Click to restore the quarantined file. A confirmation dialog box displays. You can select *Yes* to add this file/folder to the exclusion list, *No* to restore the file, or *Cancel* to exit the operation. Press and hold the Ctrl key to restore multiple entries.
Delete		Click to delete the quarantined file. A confirmation dialog box displays. Select *Yes* to continue. Press and hold the Ctrl key to delete multiple entries.
Close		Click to close the page and return to FortiClient Console.

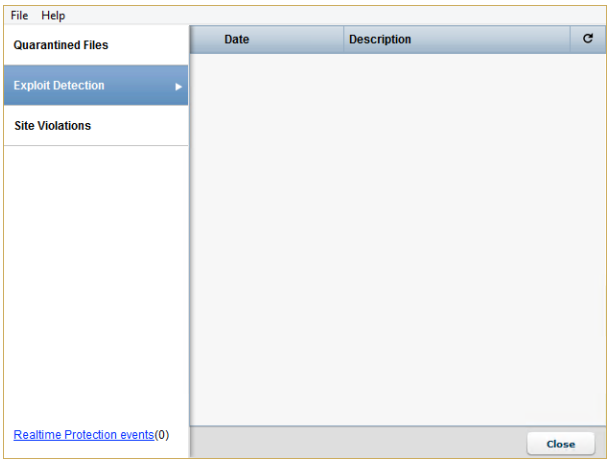
3. Click *Close*.

Viewing detected exploit attempts

You can view the exploit attempts FortiClient has blocked. See Enabling and disabling exploit prevention on page 94.

To view detected exploit attempts:

1. On the *AntiVirus* tab, click the *X Threats Detected* link
2. Click the *Exploit Detection* tab.
   In this page you can view the date and description of a blocked exploit attempt.



This page displays the following information:

Date	Date of the detected exploit attempt.

Description	Description of the exploit attempt.
Refresh	Click to refresh the list of detected exploit attempts.
Close	Click to close the page and return to FortiClient Console.

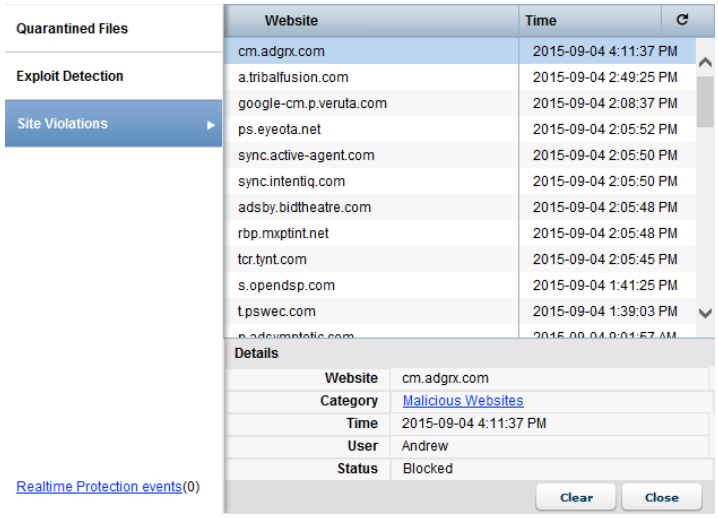
3. Click *Close*.

Viewing site violations

On the *Site Violations* page, you can view site violations and submit sites to be recategorized.

To view site violations:

1. On the *AntiVirus* tab, click *X Threats Detected*.
2. Click the *Site Violations* tab.



This *Site Violations* page displays the following options:

Website	Website name.
Time	Date and time of the site violation.
Refresh	Select to refresh the site violation list.
Details	Select an entry in the list to view site violation details, including the website name, category, date and time, username, and status. Select the category link to request to have the site category reevaluated.

3. Click *Close*.

Viewing alerts

When FortiClient antivirus detects a virus while attempting to download a file via a web browser, a warning displays.

Select *View recently detected virus(es)* to collapse the virus list. Right-click a file in the list to access the following context menu:

Delete	Delete a quarantined or restored file.
Quarantine	Quarantine a restored file.
Restore	Restore a quarantined file.
Submit Suspicious File	Submit a file to FortiGuard as a suspicious file.
Submit as False Positive	Submit a quarantined file to FortiGuard as a false positive.
Add to Exclusion List	Add a restored file to the exclusion list. Any files in the exclusion list are not scanned.
Open File Location	Open the file location on your workstation.

You must select *Alert when viruses are detected* under *AntiVirus Options* on the *Settings* page to receive the virus alert dialog box when attempting to download a virus in a web browser. If *Alert when viruses are detected* is disabled, the virus alert dialog box does not display when you attempt to download a virus in a web browser.

Viewing realtime protection events

When an antivirus realtime protection event has occurred, you can view these events in FortiClient Console.

To view realtime protection events:

1. From the *AntiVirus* tab, select *X Threats Detected*.
2. Select *Real-time Protection events (x)* in the left pane.
   The `realtime_scan.log` opens in the default viewer.
   Example log output:

```
Realtime scan result:
time: 09/29/15 10:46:07, virus found: EICAR_TEST_FILE, action: Quarantined,
      c:\users\user\desktop\eicar.com
time: 09/29/15 10:46:07, virus found: EICAR_TEST_FILE, action: Quarantined,
      c:\users\user\desktop\eicar.com.txt
time: 09/29/15 10:46:07, virus found: EICAR_TEST_FILE, action: Quarantined,
      c:\users\user\desktop\eicarcom2.zip
time: 09/29/15 10:46:08, virus found: EICAR_TEST_FILE, action: Quarantined,
      c:\users\user\desktop\eicar_com.zip
time: 09/29/15 10:46:39, virus found: EICAR_TEST_FILE, action: Quarantined,
      c:\users\user\appdata\local\temp\3g_bl8y9.com.part
time: 03/18/15 10:48:13, virus found: EICAR_TEST_FILE, action: Quarantined,
      c:\users\user\appdata\local\temp\xntwh8q1.zip.part
```

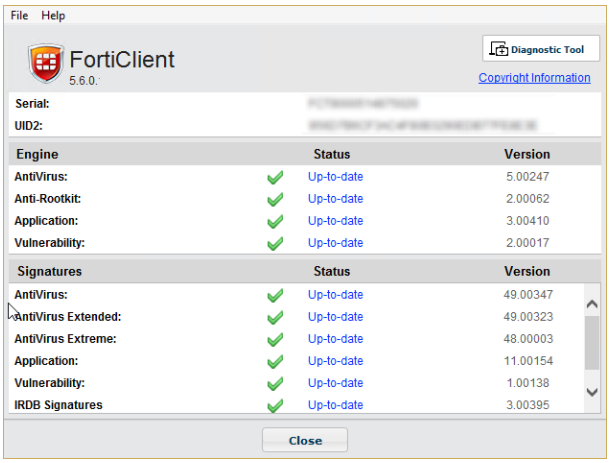
Viewing FortiClient engine and signature versions

You can view the current FortiClient version, engine, and signature information.

When EMS manages FortiClient, you can select to use a FortiManager device for FortiClient software and signature updates. When configuring the profile using EMS, select *Use FortiManager for client software/signature updates* to enable the feature, and enter the IP address of your FortiManager device. You can select to failover to FDN when FortiManager is unavailable.

To view FortiClient engine and signature versions:

1. Go to *Help* > *About*.

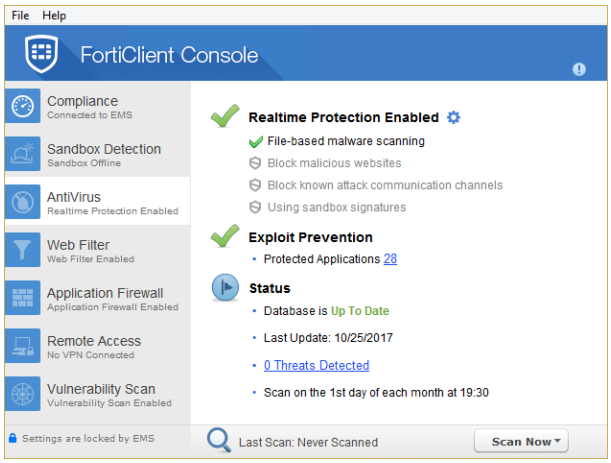


2. Hover the mouse over the *Status* field to see the date and time FortiClient last updated the selected item.
3. Click *Close*.

Protecting applications from exploits

The anti-exploit detection feature helps protect vulnerable endpoints from unknown exploit attacks. FortiClient monitors the behavior of popular applications, such as web browsers (Internet Explorer, Chrome, Firefox, Opera), Java/Flash plug-ins, Microsoft Office applications, and PDF readers, against exploits that use zero-day or unpatched vulnerabilities to infect the endpoint. Once detected, the compromised application process is terminated. The anti-exploit detection feature also helps protect against memory-based attacks and drive-by download attacks. It also detects and blocks unknown and known exploit kits. It is a signature-less solution.

You can view the number and list of applications that FortiClient is protecting from evasive exploits. On the *AntiVirus* tab, under *Exploit Prevention*, the number of protected applications displays as a link. You can click the link to view the list of application names.



The anti-exploit detection feature is available only for FortiClient (Windows).

Enabling and disabling exploit prevention

You can enable and disable exploit prevention if EMS has not locked FortiClient Console. See Protecting applications from exploits on page 93.

To enable and disable exploit prevention:

1. On the *AntiVirus* tab, click the *Settings* icon.
   The settings page displays.
2. Select the *Enable exploit prevention* checkbox to enable exploit prevention.
   Clear the *Enable exploit prevention* checkbox to disable exploit prevention.
3. Click *OK*.

Viewing applications protected from exploits

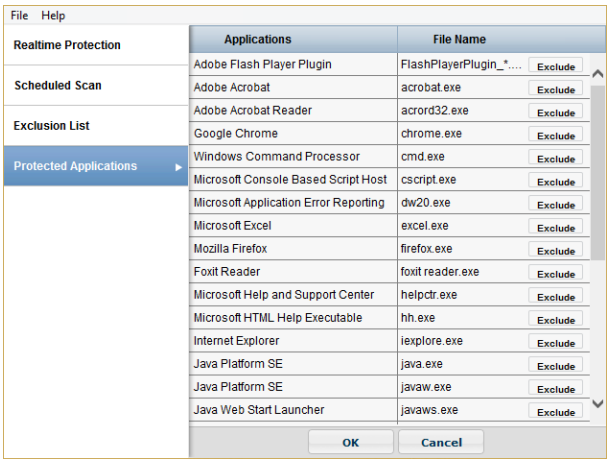
When you view the list of applications, you can use the following button names to determine which applications are protected from exploits:

- The applications with an *Exclude* button beside their names are protected from evasive exploits.
- The applications with a *Support* button beside their names are not protected from evasive exploits. You can protect the application by clicking the *Support* button. See Excluding applications from protection on page 95.

See Viewing detected exploit attempts on page 90.

To view protected applications:

1. From the *AntiVirus* tab, click the *<number>* link under *Exploit Prevention*.
   The list of protected applications displays.



2. Click *OK*.

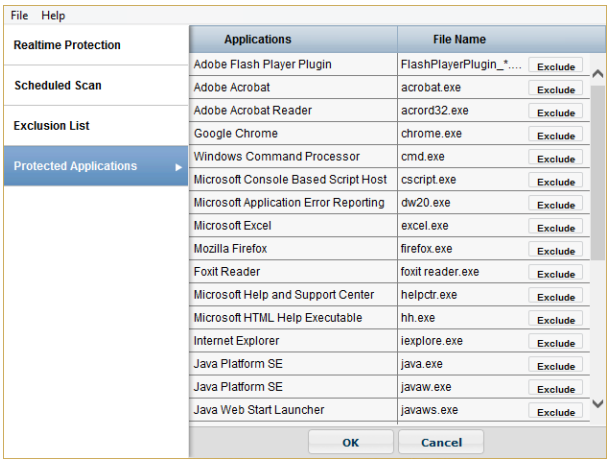
Excluding applications from protection

You can exclude applications from the list of software protected from evasive exploits. You can also add excluded applications back to the list of protected software.

For FortiClient in managed mode, when FortiClient Telemetry is connected to FortiGate or EMS, an administrator may lock the list of protected applications. You can exclude applications from protection if EMS has not locked FortiClient Console.

To exclude applications from protection:

1. On the *AntiVirus* tab, click the *Settings* icon.
2. Click the *Protected Applications* tab.
   The list of protected applications displays.



3. Beside each application you want to exclude, click *Exclude*.
   The application is excluded, and the button name changes to *Support*. Click *Support* to protect the application again.
4. Click *OK*.

Evaluating the anti-exploit detection feature

The anti-exploit detection feature blocks malicious content from exploiting vulnerabilities in applications. To test or verify this feature, you can use the Metasploit Framework module at https://www.rapid7.com/db/modules/exploit/multi/browser/adobe_flash_hacking_team_uaf. This module requires Windows 7 x86, Firefox, and Adobe Flash Player.

Consider running the exploit with and without enabling the anti-exploit detection feature in FortiClient. FortiClient blocks such an exploit and displays a bubble message in FortiTray to notify the endpoint user.

In newer product versions, vendors resolve most publicly announced exploits. The FortiClient Vulnerability Scan feature can identify, report, and apply patches for supported applications. See Vulnerability Scan on page 123.

Web Security/Web Filter

Web Security/Web Filter allows you to block, allow, warn, and monitor web traffic based on URL category or custom URL filters. FortiGuard Distribution Network (FDN) handles URL categorization. You can create a custom URL filter exclusion list that overrides the FDN category.

When FortiClient is in standalone mode, the *Web Security* tab displays. When FortiClient is in managed mode and FortiClient Telemetry is connected to FortiGate or EMS, the *Web Security* tab changes to the *Web Filter* tab.

Web Security

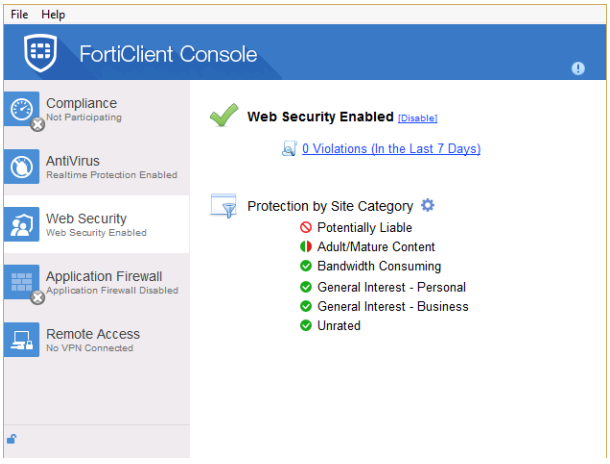
The *Web Security* tab displays in FortiClient Console when FortiClient is installed with *Additional Security Features* and *Web Filtering* selected, and FortiClient is running in standalone mode.

Enabling Web Security

You can enable Web Security when FortiClient is running in standalone mode.

To enable Web Security:

1. On the *Web Security* tab, click the *Enable* link in FortiClient Console.



The following options are available:

Enable/Disable	Select to enable or disable Web Security.
X Violations (In the Last 7 Days)	Select to view Web Security log entries of the violations that have occurred in the last seven days.
Protection by Site Category	Displays the settings and a *Settings* icon. Click the *Settings* icon to configure the site categories, exclusion list, and settings. You can also view violations.

Disabling Web Security

You can disable Web Security when FortiClient is running in standalone mode.

To disable Web Security:

1. On the *Web Security* tab, toggle the *Disable* link in FortiClient Console.

Web Filter

The *Web Filter* tab displays in FortiClient Console when FortiClient is installed with *Additional Security Features* and *Web Filtering* selected, and FortiClient Telemetry is connected to FortiGate or EMS.

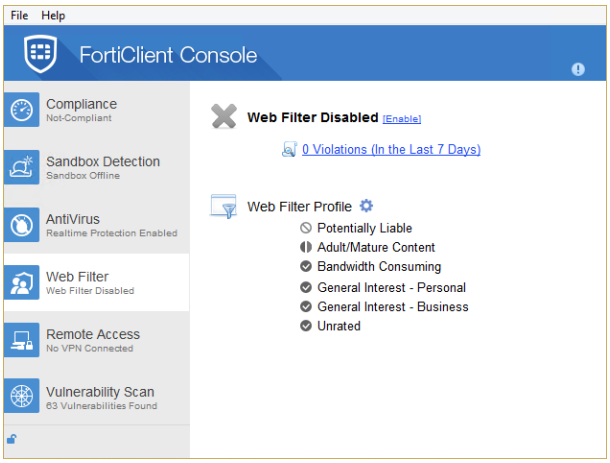
Enabling Web Filter

For FortiClient in managed mode, when FortiClient Telemetry is connected to a FortiGate or EMS, an administrator may enable, configure, and lock the web filter settings.

You can enable web filtering when EMS has not locked FortiClient Console and web filtering is excluded from FortiGate compliance rules.

To enable web filtering:

1. On the *Web Filter* tab, click *Enable* in FortiClient Console.



The following options are available:

Enable/Disable	Enable or disable Web Filter.
X Violations (In the Last 7 Days)	View Web Filter log entries of the violations that have occurred in the last seven days.
Web Filter Profile	Displays the Web Filter profile settings and a *Settings* icon. Click the *Settings* icon to configure the site categories, exclusion list, and settings. You can also view violations.

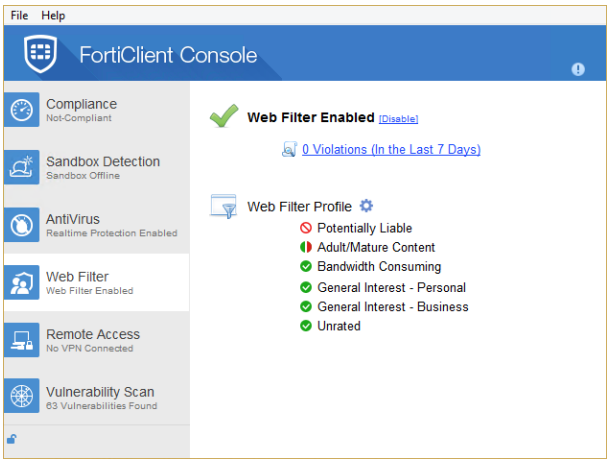
Disabling Web Filter

When FortiClient Telemetry is connected to FortiGate or EMS, you may be unable to disable web filtering.

You can disable web filtering if EMS has not locked FortiClient Console and web filtering is excluded from FortiGate compliance rules.

To disable web filtering:

1. On the *Web Filter* tab, click *Disable*.



Configuring web filtering

You can configure web filtering settings, profiles, and exclusion lists.

When FortiClient Telemetry is connected to FortiGate or EMS, you may be unable to configure web filtering.

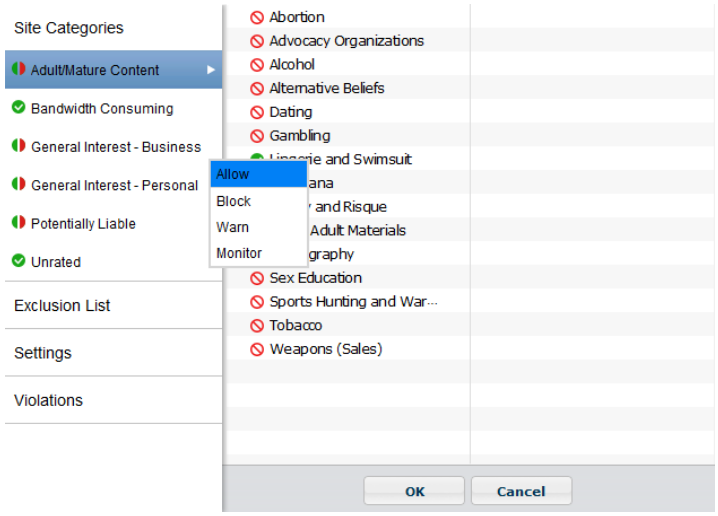
Configuring site categories

You can configure FortiClient to allow, block, warn, or monitor web traffic based on site categories.

To configure site categories:

1. On the *Web Security/Web Filter* tab, click the *Settings* icon.
2. Click a site category.

3. Click the *Action* icon, and select an action in the dropdown list.



The following actions are available:

Allow	Set the category or sub-category to *Allow* to allow access.
Block	Set the category or sub-category to *Block* to block access. The user receives a *Web Page Blocked* message in the web browser.
Warn	Set the category or sub-category to *Warn* but allow access. The user receives a *Web Page Warning* message in the web browser. The user can proceed or go back to the previous web page.
Monitor	Set the category or sub-category to *Monitor* to allow access. The site is logged.

You can enable or disable *Site Categories* in the *Web Security/Web Filter* settings page. When site categories are disabled, the exclusion list protects FortiClient.

4. Click *OK*.

Managing the Web Filter/Web Security exclusion list

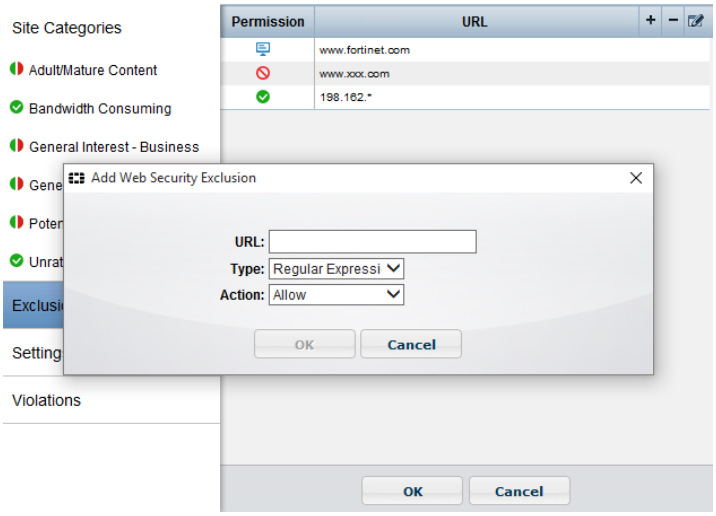
You can add websites to the exclusion list and set the permission to allow, block, monitor, or exempt.

For information on URL formats, type, and action, see the *FortiOS Handbook* in the Fortinet Document Library.

To add items to the exclusion list:

1. On the *Web Security/Web Filter* tab, click the *Settings* icon.
2. Click the *Exclusion List* tab.

3. Click the + icon to add URLs to the exclusion list.
   If the website is part of a blocked category, an allow permission in the *Exclusion List* would allow the user to access the specific URL.



4. Configure the following settings:

Exclusion List		Select to exclude URLs that are explicitly blocked or allowed. Use the add icon to add URLs and the delete icon to delete URLs from the list. Select a URL and select the edit icon to edit the selection.
	URL	Enter a URL or IP address.
	Type	Select one of the following pattern types: • *Simple* • *Wildcard* • *Regular Expression*
	Actions	Select one of the following actions: • *Block*: Block access to the website regardless of the URL category or sub-category action. • *Allow*: Allow access to the website regardless of the URL category or sub-category action. • *Monitor*: Allow access to the website regardless of the URL category or sub-category action. A log message is generated each time a matching traffic session is established.

5. Click *OK*.

To edit items in the exclusion list:

1. On the *Web Security/Web Filter* tab, click the *Settings* icon.
   The Settings page displays.
2. Click the *Exclusion List* tab.
   The exclusion list displays.

3. Click an item, and click the *Edit* icon.
   The Edit dialog box displays.
4. Edit the settings and click *OK* to save the changes.

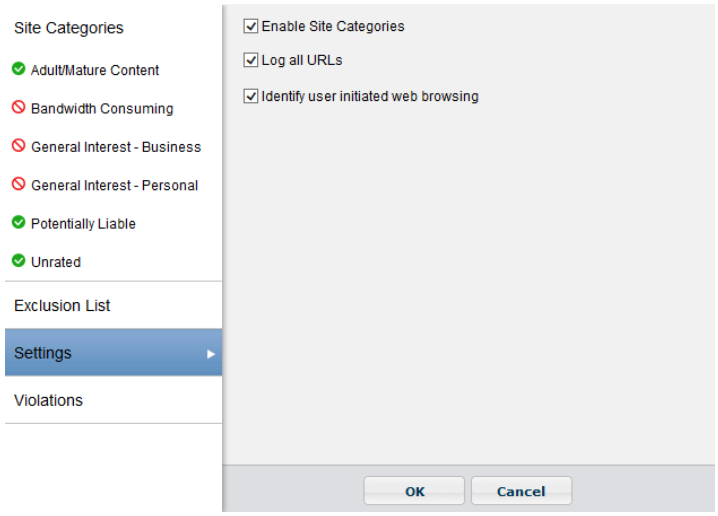
To remove items from the exclusion list:

1. On the *Web Security/Web Filter* tab, click the *Settings* icon.
   The Settings page displays.
2. Click the *Exclusion List* tab.
   The exclusion list displays.
3. Click one or more items in the exclusion list.
   A checkmark displays beside the selected items.
4. Click the - icon.
   The selected items are removed from the exclusion list.
5. Click *OK* to save the changes.

Configuring settings

To configure settings:

1. On the *Web Security/Web Filter* tab, click the *Settings* icon.
2. Click the *Settings* tab.



3. Configure the following settings:

Enable Site Categories	Select to enable site categories. When site categories are disabled, the exclusion list protects FortiClient.
Log all URLs	Select to log all URLs.
Identify user initiated web browsing	Select to identify web browsing that is user-initiated.

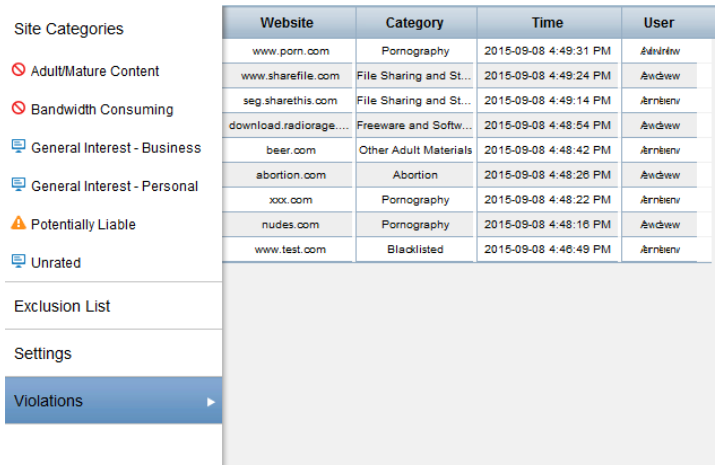
4. Click *OK*.

Viewing violations

You can view web filtering violations in FortiClient Console.

To view violations:

1. On the *Web Security/Web Filter* tab, click the *Settings* icon. Alternately, you can click the *X Violations (In the Last 7 Days)* link.
2. Click the *Violations* tab.



The following information displays.

Website	Website name or IP address.
Category	Website sub-category.
Time	Date and time the website was accessed.
User	Name of the user generating the traffic. Hover the cursor over the column to view the complete entry in the popup bubble message.

3. Click *Close*.

Application Firewall

This section applies only to FortiClient in managed mode.

FortiClient can recognize the traffic generated by a large number of applications. You can create rules to block or allow traffic per category or application.

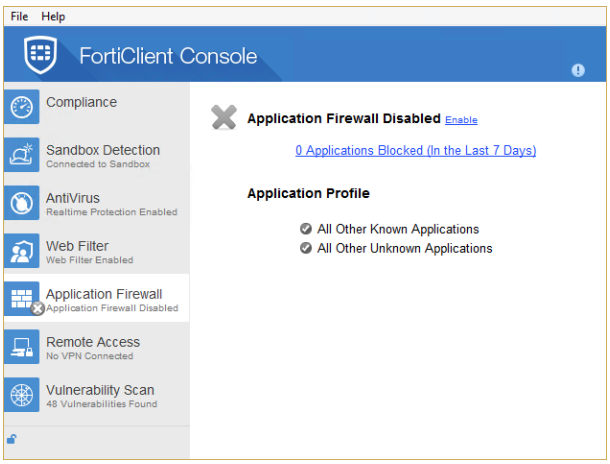
Enabling Application Firewall

The *Application Firewall* tab displays in FortiClient Console when FortiClient is installed with *Additional Security Features* and *Application Firewall* selected.

For FortiClient in managed mode, when FortiClient Telemetry is connected to FortiGate or EMS, an administrator may enable, configure, and lock the application firewall settings. You can enable *Application Firewall* when EMS has not locked the settings.

To enable Application Firewall:

1. On the *Application Firewall* tab, click the *Enable* link.



4. If prompted, click *Elevate*.

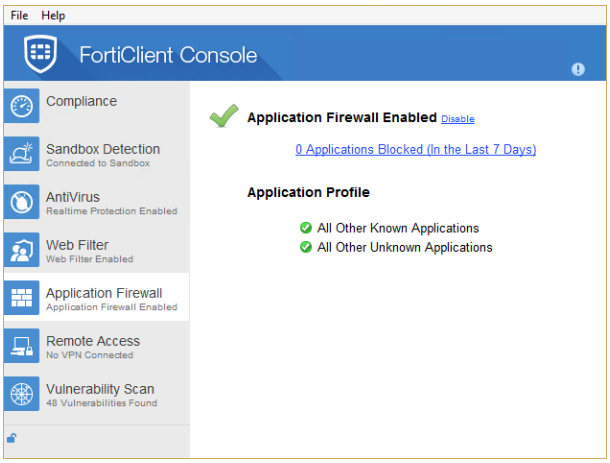
Application Firewall is enabled.

Disabling Application Firewall

When FortiClient Telemetry is connected to FortiGate, you may be unable to disable application firewall. You can disable *Application Firewall* when EMS has not locked the settings.

To disable Application Firewall:

1. On the *Application Firewall* tab, click the *Disable* link.



Application Firewall is disabled.

Viewing blocked applications

To view blocked applications:

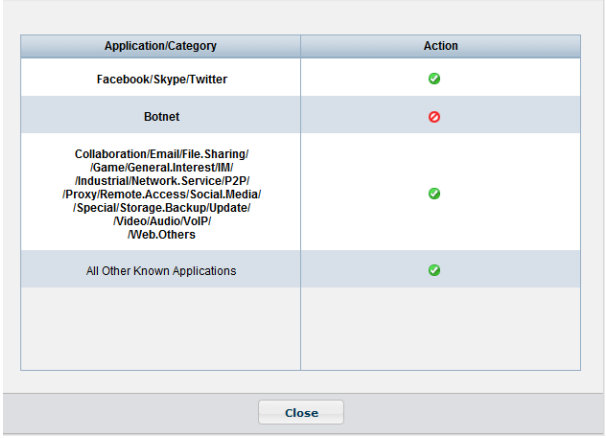
1. On the *Application Firewall* tab, click the *<number> Applications Blocked (In the Last 7 Days)* link.
   A page of all blocked applications blocked applications displays.

Viewing application firewall profiles

You can view the application firewall profile when FortiClient Telemetry is connected to EMS.

To view the application firewall profile:

1. On the *Application Firewall* tab, click *Show all*.



Remote Access

FortiClient supports both IPsec and SSL VPN connections to your network for remote access. Administrators can use EMS to provision VPN configurations for FortiClient Console and endpoint users can configure new VPN connections using FortiClient Console.

Enabling remote access

The *Remote Access* tab displays in FortiClient Console when FortiClient is installed with *Secure Remote Access* selected.

When FortiClient is in managed mode and managed by EMS, FortiClient may include VPN connection configurations for you to use.

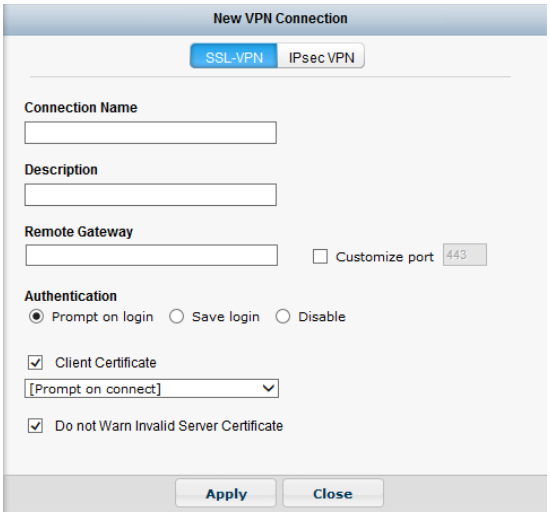
Configuring VPN connections

You can configure SSL VPN connections and IPsec VPN connections using FortiClient Console.

Configuring SSL VPN connections

To configure SSL VPN connections:

1. On the *Remote Access* tab, click the *Configure VPN* link or use the dropdown link in FortiClient Console.



2. Select *SSL-VPN*, then configure the following settings:

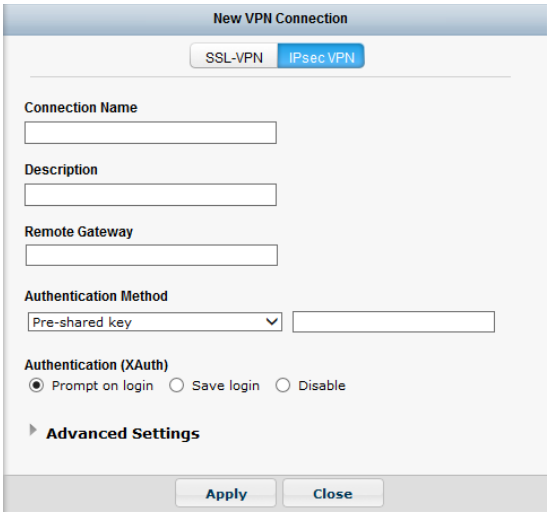
Connection Name	Enter a name for the connection.
Description	(Optional) Enter a description for the connection.
Remote Gateway	Enter the IP address/hostname of the remote gateway. Multiple remote gateways can be configured by separating each entry with a semicolon. If one gateway is not available, the VPN connects to the next configured gateway.
Customize port	Select to change the port. The default port is 443.
Authentication	Select to *Prompt on login* or *Save login*. The *Disable* option is available when *Client Certificate* is enabled.
Username	If you selected *Save login*, type the username to save for the login.
Client Certificate	Select to enable client certificates, then select *Prompt on connect* or the certificate from the dropdown list.
Do not Warn Invalid Server Certificate	Select if you do not want to be warned if the server presents an invalid certificate.
+	Select the add icon to add a new connection.
-	Select a connection and then select the delete icon to delete a connection.

3. Click *Apply* to save the VPN connection, and then click *Close* to return to the *Remote Access* screen.

Configuring IPsec VPN connections

To configure IPsec VPN connections:

1. On the *Remote Access* tab, click the *Configure VPN* link, or use the dropdown list in FortiClient Console.



2. Select *IPsec VPN*, then configure the following settings:

Connection Name	Enter a name for the connection.
Description	(Optional) Enter a description for the connection.
Remote Gateway	Enter the IP address/hostname of the remote gateway. Multiple remote gateways can be configured by separating each entry with a semicolon. If one gateway is not available, the VPN connects to the next configured gateway.
Authentication Method	Select *X.509 Certificate* or *Pre-shared Key* in the dropdown list. When you select *x.509 Certificate*, select *Prompt on connect* or a certificate from the list.
Authentication (XAuth)	Select *Prompt on login*, *Save login*, or *Disable*.
Username	If you selected *Save login*, type the username to save for the login.
Advanced Settings	Configure VPN settings, phase 1, and phase 2 settings.
VPN Settings	
Mode	Select one of the following: • *Main*: In main mode, the phase 1 parameters are exchanged in multiple rounds with encrypted authentication information. • *Aggressive*: In aggressive mode, the phase 1 parameters are exchanged in a single message with authentication information that is not encrypted. Although *Main* mode is more secure, you must select *Aggressive* mode if there is more than one dialup phase 1 configuration for the interface IP address, and the remote VPN peer or client is authenticated using an identifier (local ID).
Options	Select one of the following: • *Mode Config*: IKE Mode Config can configure host IP address, domain, DNS and WINS addresses. • *Manually Set*: Manual key configuration. If one of the VPN devices is manually keyed, the other VPN device must also be manually keyed with the identical authentication and encryption keys. Enter the DNS server IP, assign IP address, and subnet values. Select the checkbox to enable split tunneling. • *DHCP over IPsec*: DHCP over IPsec can assign an IP address, domain, DNS and WINS addresses. Select the checkbox to enable split tunneling.

Phase 1		Select the encryption and authentication algorithms used to generate keys for protecting negotiations and add encryption and authentication algorithms as required. You need to select a minimum of one and a maximum of two combinations. The remote peer or client must be configured to use at least one of the proposals that you define.
	IKE Proposal	Select symmetric-key algorithms (encryption) and message digests (authentication) from the dropdown lists.
	DH Group	Select one or more Diffie-Hellman groups from DH group 1, 2, 5, 14, 15, 16, 17, 18, 19 and 20. At least one of the DH group settings on the remote peer or client must match one the selections on the FortiGate unit. Failure to match one or more DH groups will result in failed negotiations.
	Key Life	Enter the time (in seconds) that must pass before the IKE encryption key expires. When the key expires, a new key is generated without interrupting service. The key life can be from 120 to 172,800 seconds.
	Local ID	Enter the local ID (optional). This local ID value must match the peer ID value given for the remote VPN peer's peer options.
	Dead Peer Detection	Select this checkbox to reestablish VPN tunnels on idle connections and clean up dead IKE peers if required.
	NAT Traversal	Select the checkbox if a NAT device exists between the client and the local FortiGate unit. The client and the local FortiGate unit must have the same NAT traversal setting (both selected or both cleared) to connect reliably.
Phase 2		Select the encryption and authentication algorithms that will be proposed to the remote VPN peer. You can specify up to two proposals. To establish a VPN connection, at least one of the proposals you specify must match configuration on the remote peer.
	IKE Proposal	Select symmetric-key algorithms (encryption) and message digests (authentication) from the dropdown lists.
	Key Life	The *Key Life* setting sets a limit on the length of time that a phase 2 key can be used. The default units are seconds. Alternatively, you can set a limit on the number of kilobytes (KB) of processed data, or both. If you select both, the key expires when the time has passed or the number of KB have been processed. When the phase 2 key expires, a new key is generated without interrupting service.
	Enable Replay Detection	Replay detection enables the unit to check all IPsec packets to see if they have been received before. If any encrypted packets arrive out of order, the unit discards them.

	Enable Perfect Forward Secrecy (PFS)	Select the checkbox to enable perfect forward secrecy (PFS). PFS forces a new Diffie-Hellman exchange when the tunnel starts and whenever the phase 2 key life expires, causing a new key to be generated each time.
	DH Group	Select one Diffie-Hellman (DH) group (1, 2, 5, 14, 15, 16, 17, 18, 19 or 20). This must match the DH group the remote peer or dialup client uses.
+		Select the add icon to add a new connection.
-		Select a connection and then select the delete icon to delete a connection.

3. Click *Apply* to save the VPN connection, and then click *Close* to return to the Remote Access screen.

Connecting VPNs

You can connect VPN tunnels to FortiGate.

Connecting SSL and IPsec VPNs

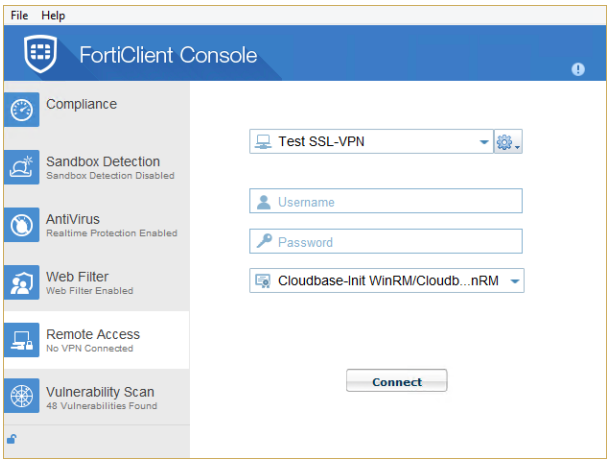
Depending on the FortiClient configuration, you may also have permission to edit an existing VPN connection and delete an existing VPN connection.

Microsoft Internet Explorer's SSL and TLS settings should be the same as those on the FortiGate.

To connect to VPNs:

1. On the *Remote Access* tab, select the VPN connection from the dropdown list.
   Optionally, you can click the system tray, right-click the icon, and select a VPN configuration to connect.

Provisioned VPN connections are listed under *Corporate VPN*. Locally configured VPN connections are listed under *Personal VPN*.



2. Type your username and password.
3. If a certificate is required, select a certificate.

   If the VPN tunnel was configured to require a certificate, you must select a certificate. If no certificate is required, the option is hidden in FortiClient Console.

   Your administrator may have configure FortiClient to automatically locate a certificate for you.
4. Click the *Connect* button.

   When connected, FortiClient Console displays the connection status, duration, and other relevant information. You can now browse your remote network. Click the *Disconnect* button when you are ready to terminate the VPN session.

Connecting VPNs with FortiToken Mobile

VPN connections to FortiGate may require network authentication that uses a token from FortiToken Mobile, which is an application that runs on Android or iOS devices. For information about FortiToken Mobile, see the Document Library.

FortiGate can be configured to let you push a token from FortiClient Console to FortiGate to complete network authentication when connecting VPNs. When configured, you can push the token by clicking the *FTM Push* button in FortiClient Console. The push token is sent to FortiGate, and you receive a notification of the authentication request on your device that has FortiToken Mobile installed. On your device, you can tap the notification and follow the instructions to allow or deny the authentication request.

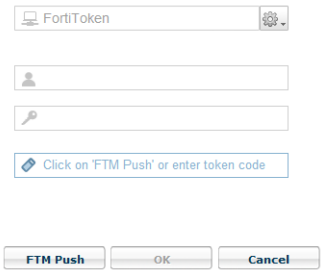
If a push token is not configured, you must type a token code from FortiToken Mobile into FortiClient Console when connecting VPNs.

You must have available the device with FortiToken Mobile installed to complete this procedure.

To connect VPNs with FortiToken Mobile using push notifications:

1. On the *Remote Access* tab, select the VPN connection from the dropdown list.
2. Enter your username and password and click the *Connect* button.

   The *Click on 'FTM Push' or enter token code* box displays.



3. Click *FTM Push*.
   Your device with FortiToken Mobile installed receives a notification.
4. On your device with FortiToken Mobile installed, tap the notification and follow the instructions to allow the authentication request and complete network authentication without typing the token code.
   You can also deny the authentication request, or do nothing and let the notification request expire.

To connect VPNs with FortiToken Mobile by typing token codes:

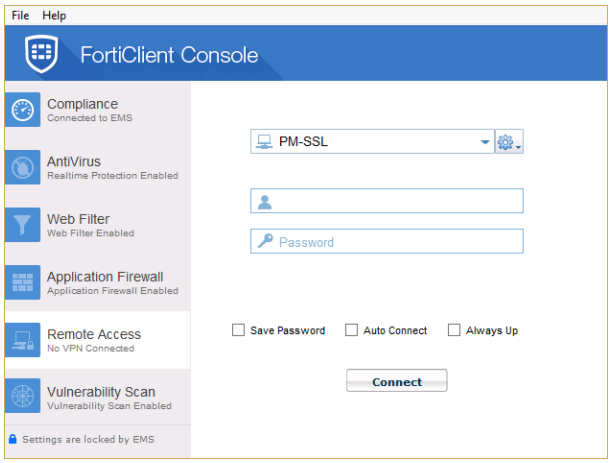
1. On the *Remote Access* tab, select the VPN connection from the dropdown list.
2. Enter your username and password and click the *Connect* button.
   The *Enter token code* box displays.
3. Type the token code from your FortiToken Mobile and click *OK* to complete network authentication.

Save password, auto connect, and always up

When an administrator uses EMS to configure a profile for FortiClient, the administrator can configure an IPsec or SSL VPN connection to FortiGate and enable the following features:

- *Save Password*: Allows the user to save the VPN connection password in the console.
- *Auto Connect*: When FortiClient is launched, the VPN connection automatically connects.
- *Always Up (Keep Alive)*: When selected, the VPN connection is always up, even when no data is being processed. If the connection fails, keep alive packets sent to the FortiGate sense when the VPN connection is available and reconnect VPN.

After FortiClient Telemetry connects to FortiGate when FortiGate and EMS are integrated, FortiClient receives a profile from EMS that contains IPsec and/or SSL VPN connections to FortiGate. The following example shows an SSL VPN connection named *PM-SSL*.



If the VPN connection fails, a popup displays to inform you about the connection failure while FortiClient continues trying to reconnect VPN in the background.

Depending on the VPN configuration, the popup may include a *Cancel* button. If you click the *Cancel* button, FortiClient stops trying to reconnect VPN.

Access to certificates in Windows Certificates Stores

On a Windows system, you can view certificates by using an MMC (Microsoft Management Console) snap-in called Certificates console. For more information, see the following Microsoft TechNet articles:

- *Add the Certificates Snap-in to an MMC* available at https://technet.microsoft.com/en-us/library/cc754431
- *Display Certificate Stores* available at https://technet.microsoft.com/en-us/library/cc725751

The Certificates console offers the following snap-in options:

- My user account
- Service account
- Computer account

You can select one or more snap-in options, and they will display in the Certificates console. FortiClient typically searches for certificates in one of the following accounts:

- User account – contains certificates for the logged on user
- Computer account – contains certificates for the local computer

If the certificate is in the local computer account, FortiClient can typically access the certificate. A certificate from the local computer account may be used to establish an IPsec VPN connection, regardless of whether the logged on user is an administrator or a non-administrator. For SSL VPN, the administrator needs to grant permission to users who are non-administrators to access the private key of the certificate. Otherwise, non-administrators cannot use the certificate in the computer account to establish SSL VPN connections. This restriction does not apply to any user with administrator level permission. IPsec VPN does not have this exception.

If the certificate is in the user account, FortiClient can access the certificate, if the user has already successfully logged in, and the same user imported the certificate. In all other scenarios, FortiClient may be unable to access the certificate.

The following table summarizes when FortiClient can (yes) and cannot (no) locate the certificate for users who are logged into the endpoint and connecting VPN tunnels:

Account	Connect VPN using FortiClient GUI or FortiTray	
	Logged in user with admin privilege	Logged in user with non-admin privilege
User account	Yes, certificate found, if the same administrator user imported the certificate	Yes, certificate found, if the same user imported the certificate
Computer account	Yes, certificate found	IPsec VPN: Yes, certificate found SSL VPN: Yes, certificate found, if access permission granted to private key
SmartCard	Yes, certificate found, if same user that was logged on at the time card was inserted	Yes, certificate found, if same user that was logged on at the time card was inserted

When a user imports a certificate into the user account, a different logged on user cannot access the same certificate.

A certificate on a smart card is imported into the user account of the logged on user. As a result, the same conditions apply as with the user account.

The following table summarizes when FortiClient can (yes) and cannot (no) locate the certificate before a user logs into the endpoint:

Account	Unknown user before logging into Windows
User account	No certificate found
Computer account	Yes certificate found
SmartCard	No certificate found

Advanced features (Microsoft Windows)

When deploying a custom FortiClient XML configuration, use the advanced FortiClient profile options in EMS to ensure the FortiClient profile settings do not overwrite your custom XML settings. For information, see the *FortiClient XML Reference*.

Activating VPN before Windows log on

When using VPN before Windows log on, the user is offered a list of preconfigured VPN connections to select from on the Windows log on screen. This requires that the Windows log on screen is not bypassed. As such, if VPN before Windows log on is enabled, it is required to also select the *Users must enter a user name and password to use this computer* checkbox in the *User Accounts* dialog box.

To make this change, proceed as follows:

In FortiClient:

1. Create the VPN tunnels of interest or connect to FortiClient EMS, which provides the VPN list of interest
2. Enable VPN before log on to the FortiClient Settings page, see VPN options on page 133.

On the Microsoft Windows system,

1. Start an elevated command line prompt.
2. Enter `control passwords2` and press `Enter`. Alternatively, you can enter `netplwiz`.
3. Check the checkbox for *Users must enter a user name and password to use this computer*.
4. Click *OK* to save the setting.

Connecting VPNs before logging on (AD environments)

The VPN `<options>` tag holds global information controlling VPN states. The VPN connects first, then logs on to AD/domain.

```
<forticlient_configuration>
   <vpn>
      <options>
         <show_vpn_before_logon>1</show_vpn_before_logon>
         <use_windows_credentials>1</use_windows_credentials>
      </options>
   </vpn>
</forticlient_configuration>
           ...
           </options>
              <connections>
                 <connection>
                    <name>psk_90_1</name>
                    <type>manual</type>
                    <ike_settings>
                    <prompt_certificate>0</prompt_certificate>
                    <server>10.10.90.1;ipsecdemo.fortinet.com;172.17.61.143</server>
                    <redundantsortmethod>1</redundantsortmethod>
                    ...
              </ike_settings>
           </connection>
        </connections>
      </ipsecvpn>
   </vpn>
</forticlient_configuration>
```

This is a balanced but incomplete XML configuration fragment. All closing tags are included but some important elements to complete the IPsec VPN configuration are omitted.

RedundantSortMethod = 1

This XML tag sets the IPsec VPN connection as ping-response-based. The VPN connects to the FortiGate which responds the fastest.

RedundantSortMethod = 0

By default, RedundantSortMethod =0 and the IPsec VPN connection is priority-based. Priority-based configurations try to connect to the FortiGate starting with the first in the list.

Creating redundant IPsec VPNs

To use VPN resiliency/redundancy, configure a list of VPN gateways, instead of just one:

```
<forticlient_configuration>
   <vpn>
      <ipsecvpn>
           <options>
           ...
           </options>
              <connections>
                 <connection>
                    <name>psk_90_1</name>
                    <type>manual</type>
                    <ike_settings>
                    <prompt_certificate>0</prompt_certificate>
                    <server>10.10.90.1;ipsecdemo.fortinet.com;172.17.61.143</server>
                    <redundantsortmethod>1</redundantsortmethod>
                    ...
              </ike_settings>
           </connection>
        </connections>
      </ipsecvpn>
   </vpn>
</forticlient_configuration>
```

This is a balanced but incomplete XML configuration fragment. All closing tags are included, but some important elements to complete the IPsec VPN configuration are omitted.

RedundantSortMethod = 1

This XML tag sets the IPsec VPN connection as ping-response-based. The VPN connects to the FortiGate which responds the fastest.

RedundantSortMethod = 0

By default, RedundantSortMethod =0 and the IPsec VPN connection is priority-based. Priority-based configurations try to connect to the FortiGate starting with the first in the list.

```
        </connections>
      </sslvpn>
```

```
   </vpn>
</forticlient_configuration>
```

This is a balanced but incomplete XML configuration fragment. All closing tags are included, but some important elements to complete the SSL VPN configuration are omitted.

For SSL VPN, all FortiGates must use the same TCP port.

Creating priority-based SSL VPN connections

SSL VPN supports priority-based configurations for redundancy.

```
<forticlient_configuration>
   <vpn>
      <sslvpn>
         <options>
            <enabled>1</enabled>
            ...
         </options>
         <connections>
            <connection>
               <name>ssl_90_1</name>
               <server>10.10.90.1;ssldemo.fortinet.com;172.17.61.143:443</server>
               ...
            </connection>
         </connections>
      </sslvpn>
   </vpn>
</forticlient_configuration>
```

This is a balanced but incomplete XML configuration fragment. All closing tags are included, but some important elements to complete the SSL VPN configuration are omitted.

For SSL VPN, all FortiGates must use the same TCP port.

Advanced features (Mac OS X)

When deploying a custom FortiClient XML configuration, use the advanced FortiClient profile options in EMS to ensure the FortiClient profile settings do not overwrite your custom XML settings. See the *FortiClient XML Reference*.

Creating redundant IPsec VPNs

To use VPN resiliency/redundancy, configure a list of FortiGate or EMS IP/FQDN servers, instead of just one:

```
<forticlient_configuration>
   <vpn>
      <ipsecvpn>
            <options>
            ...
            </options>
```

```
            <connections>
               <connection>
                  <name>psk_90_1</name>
                  <type>manual</type>
                  <ike_settings>
                  <prompt_certificate>0</prompt_certificate>
                  <server>10.10.90.1;ipsecdemo.fortinet.com;172.17.61.143</server>
                  <redundantsortmethod>1</redundantsortmethod>
                  ...
               </ike_settings>
            </connection>
         </connections>
      </ipsecvpn>
   </vpn>
</forticlient_configuration>
```

This is a balanced but incomplete XML configuration fragment. All closing tags are included, but some important elements to complete the IPsec VPN configuration are omitted.

RedundantSortMethod = 1

This XML tag sets the IPsec VPN connection as ping-response-based. The VPN connects to the FortiGate or EMS which responds the fastest.

RedundantSortMethod = 0

By default, RedundantSortMethod =0 and the IPsec VPN connection is priority-based. Priority-based configurations tries to connect to the FortiGate or EMS starting with the first in the list.

```
            </connection>
         </connections>
      </sslvpn>
   </vpn>
</forticlient_configuration>
```

This is a balanced but incomplete XML configuration fragment. All closing tags are included, but some important elements to complete the SSL VPN configuration are omitted.

For SSL VPN, all FortiGate or EMS units must use the same TCP port.

Creating priority-based SSL VPN connections

SSL VPN supports priority-based configurations for redundancy.

```
<forticlient_configuration>
   <vpn>
      <sslvpn>
         <options>
            <enabled>1</enabled>
            ...
         </options>
         <connections>
            <connection>
               <name>ssl_90_1</name>
```

```
                <server>10.10.90.1;ssldemo.fortinet.com;172.17.61.143:443</server>
                ...
            </connection>
         </connections>
      </sslvpn>
   </vpn>
</forticlient_configuration>
```

This is a balanced but incomplete XML configuration fragment. All closing tags are included, but some important elements to complete the SSL VPN configuration are omitted.

For SSL VPN, all FortiGate or EMS must use the same TCP port.

VPN tunnel and script

This feature supports auto running a user-defined script after the configured VPN tunnel is connected or disconnected. The scripts are batch scripts in Windows and shell scripts in Mac OS X. They are defined as part of a VPN tunnel configuration on EMS's XML format FortiClient profile. The profile is pushed down to FortiClient from EMS. When FortiClient's VPN tunnel is connected or disconnected, the respective script defined under that tunnel is executed.

Windows

Map a network drive after tunnel connection

The script maps a network drive and copies some files after the tunnel is connected.

```
<on_connect>
   <script>
      <os>windows</os>
      <script>
         <script>
            <![CDATA[ net use x: \\192.168.10.3\ftpshare /user:Ted Mosby md c:\test copy
                 x:\PDF\*.* c:\test ]]>
         </script>
      </script>
   </script>
</on_connect>
```

Delete a network drive after tunnel is disconnected

The script deletes the network drive after the tunnel is disconnected.

```
<on_disconnect>
   <script>
      <os>windows</os>
      <script>
         <script>
            <![CDATA[ net use x: /DELETE ]]>
         </script>
      </script>
   </script>
```

```
</on_disconnect>
```

Delete a network drive after tunnel is disconnected

The script deletes the network drive after the tunnel is disconnected.

```
<on_disconnect>
   <script>
      <os>mac</os>
      <script>
         /sbin/umount /Volumes/installers
         /bin/rm -fr /Users/admin/Desktop/dropbox/*
      </script>
   </script>
</on_disconnect>
```

OS X

Map a network drive after tunnel connection

The script maps a network drive and copies some files after the tunnel is connected.

```
<on_connect>
   <script>
      <os>mac</os>
      <script>
         /bin/mkdir /Volumes/installers
         /sbin/ping -c 4 192.168.1.147 > /Users/admin/Desktop/dropbox/p.txt
         /sbin/mount -t smbfs //kimberly:RigUpTown@ssldemo.fortinet.com/installers
               /Volumes/installers/ > /Users/admin/Desktop/dropbox/m.txt
         /bin/mkdir /Users/admin/Desktop/dropbox/dir
         /bin/cp /Volumes/installers/*.log /Users/admin/Desktop/dropbox/dir/.
      </script>
   </script>
</on_connect>
```

Delete a network drive after tunnel is disconnected

The script deletes the network drive after the tunnel is disconnected.

```
<on_disconnect>
   <script>
      <os>mac</os>
      <script>
         /sbin/umount /Volumes/installers
         /bin/rm -fr /Users/admin/Desktop/dropbox/*
      </script>
   </script>
</on_disconnect>
```

Vulnerability Scan

FortiClient includes a *Vulnerability Scan* component to check endpoints for known vulnerabilities. The vulnerability scan results can include:

- List of vulnerabilities detected
- How many detected vulnerabilities are rated as critical, high, medium, or low threats
- Links to more information, including links to the FortiGuard Center (FortiGuard.com)
- One-click link to install patches and resolve as many identified vulnerabilities as possible
- List of patches that require manual installation by the endpoint user to resolve vulnerabilities

FortiClient can detect known vulnerabilities for many software. For the list of software, see Vulnerability Patches on page 143.

Compliance and vulnerability scanning

If compliance is enabled for FortiClient in managed mode, and FortiGate compliance rules require it, all automatic and manual software patches must be installed within a time frame to maintain compliant status and network access. The default time frame is one day; however, the FortiGate administrator may choose a different time frame. Contact your system administrator to learn how long you have to fix vulnerabilities. For information about compliance, see Compliance on page 49.

Enabling vulnerability scan

Vulnerability scanning is enabled by default. You cannot disable or configure the vulnerability scan feature by using the FortiClient console.

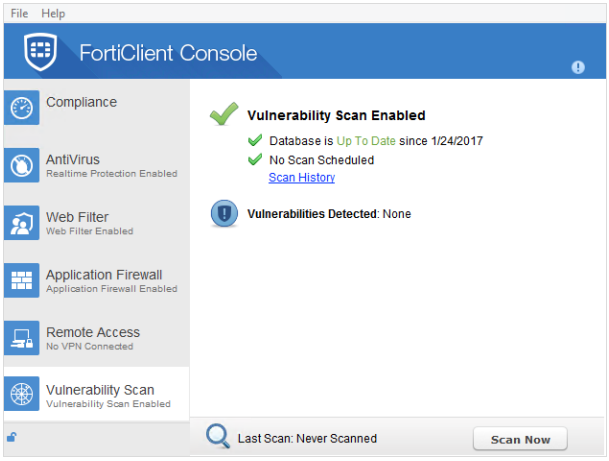
When FortiClient is in managed mode and managed by EMS, an administrator may configure and lock vulnerability scanning for you. An administrator may also disable vulnerability scanning.

Scanning now

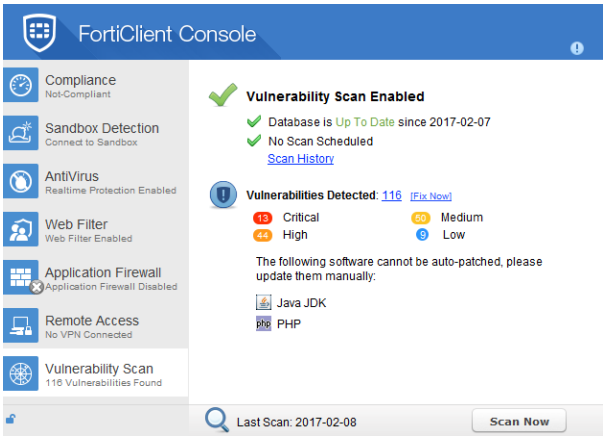
You can scan on-demand. When the scan is complete, FortiClient displays a summary of vulnerabilities found on the endpoint. If any detected vulnerabilities require you to manually install remediation patches, the list of affected software also displays.

To scan now:

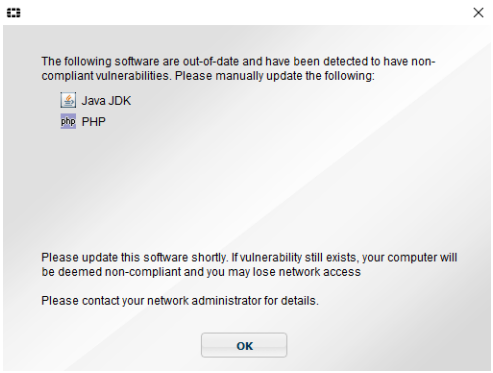
1. On the *Vulnerability Scan* tab, click the *Scan Now* button.



FortiClient scans the endpoint for known vulnerabilities, and a summary of vulnerabilities found on the system displays.



If any detected vulnerabilities require you to manually install remediation patches, a dialog box displays that informs you what software should be updated. If you fail to update the identified software, you may lose access to the network. If you lose access to the network, contact your system administrator for assistance. Following is an example of the dialog box:



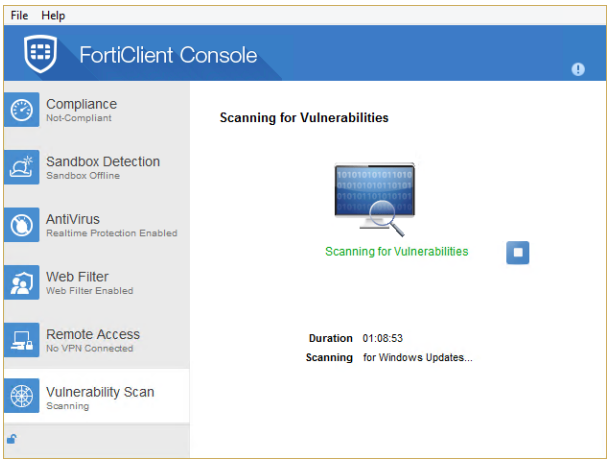
2. If applicable, read the list of software that requires manual installation of software patches, and click *OK*. See Manually fixing detected vulnerabilities on page 127.

Canceling scans

In standalone mode, when FortiClient is scanning for vulnerabilities, a *Cancel Scan* button displays, and you can click the button to cancel the scan.

To cancel a vulnerability scan:

1. On the *Vulnerability Scan* tab, click the *Cancel Scan* button.



The vulnerability scan is canceled.

Automatically fixing detected vulnerabilities

The *Vulnerability Scan* tab identifies vulnerabilities on the endpoint that should be fixed by installing software patches. You can automatically install software patches by clicking the *Fix Now* link or review detected vulnerabilities before installing software patches.

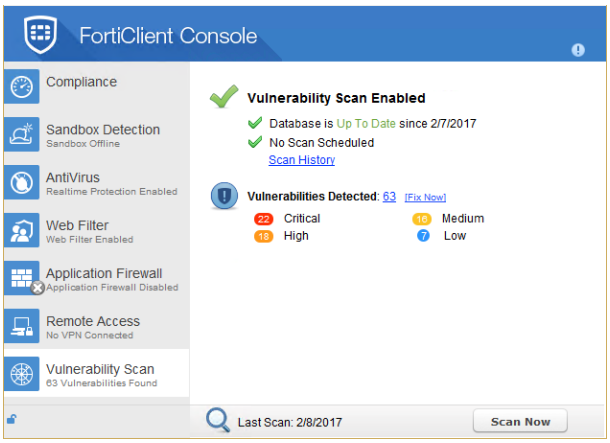
Any software patches that cannot be automatically installed are listed on the *Vulnerability Scan* tab and you should manually download and install software patches for the vulnerable software.

If compliance is enabled for FortiClient in managed mode and FortiGate compliance rules require it, all software patches must be installed within a time frame to maintain compliant status and network access. See Compliance and vulnerability scanning on page 123.

In managed mode, you may be unable to automatically fix vulnerabilities. An administrator may have the vulnerabilities automatically fixed for you.

To automatically fix detected vulnerabilities:

1. In the *Vulnerability Scan* tab, beside *Vulnerabilities Detected*, click *Fix Now* to automatically install software patches to fix the detected vulnerabilities.



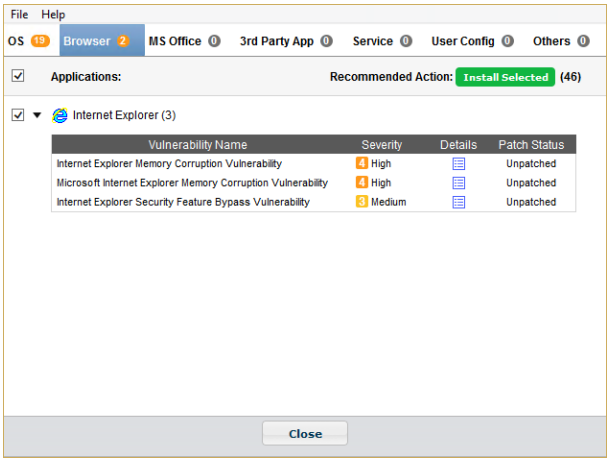
FortiClient installs the software patches. You may need to reboot the endpoint to complete installation.

Reviewing detected vulnerabilities before fixing

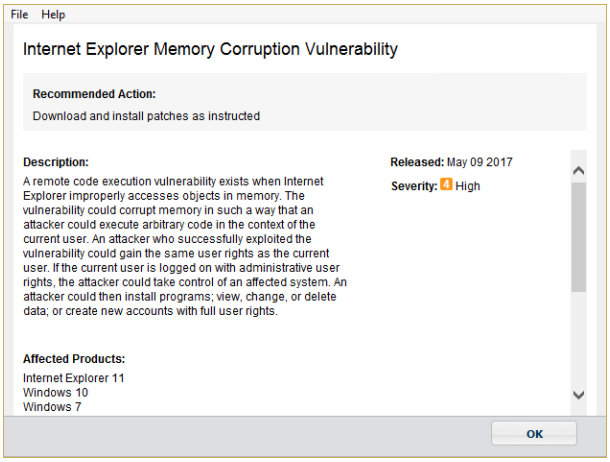
To review detected vulnerabilities before fixing:

1. In the *Vulnerability Scan* tab, beside *Vulnerabilities Detected*, click the *<number>* link to review information about vulnerabilities before installing patches.

   A page of details displays.
2. Click each category with vulnerabilities to view its details. For example, click the *Browser* category to view details about detected browser vulnerabilities.



3. Click the *Details* icon for each vulnerability to view its details and click *OK* to close the detailed view.



4. In each category, select the checkbox for the software for which you want to install patches.

   For example, in the *OS* category, expand *Operating System*, and select the checkbox beside the vulnerabilities for which you want to install patches.

   You may be unable to choose which patches to install, depending on your FortiClient configuration. You are also unable to select the checkbox for any software that requires manual installation of patches.
5. Click the *Install Selected* button to install patches.

   FortiClient installs the patches. You may need to reboot the endpoint to complete installation.

Manually fixing detected vulnerabilities

In some cases, FortiClient cannot automatically install software patches, and you must manually download and install software patches. After each scan, the *Vulnerability Scan* tab lists any software that requires you to manually download and install software patches. See also Scanning now on page 123.

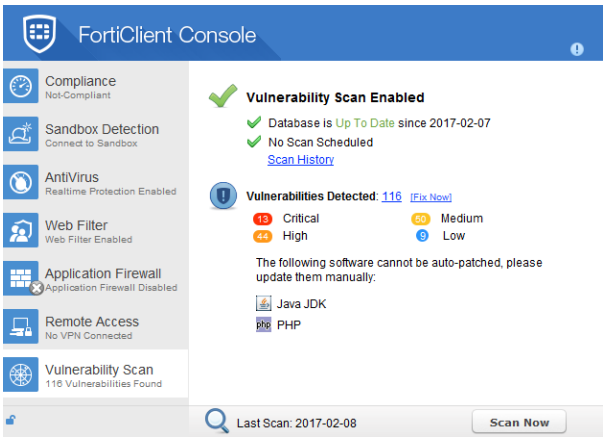
If a software vendor has ceased to provide patches for its software, the software is tagged as obsolete in the signatures used by the Vulnerability Scan feature, and you must uninstall the software to fix detected vulnerabilities. The obsolete tag is visible in the details. See Viewing details about vulnerabilities on page 128.

If compliance is enabled for FortiClient in managed mode, and FortiGate compliance rules require it, all software patches must be installed within a time frame to maintain compliant status and network access. See also Compliance and vulnerability scanning on page 123.

To manually fix detected vulnerabilities:

1. On the *Vulnerability Scan* tab, identify the software that requires manual fixing.

   Any software with detected vulnerabilities that requires you to manually download and install software patches is displayed in the *Vulnerabilities Detected* area. In the following example, Java JDK and PHP require manual updates:



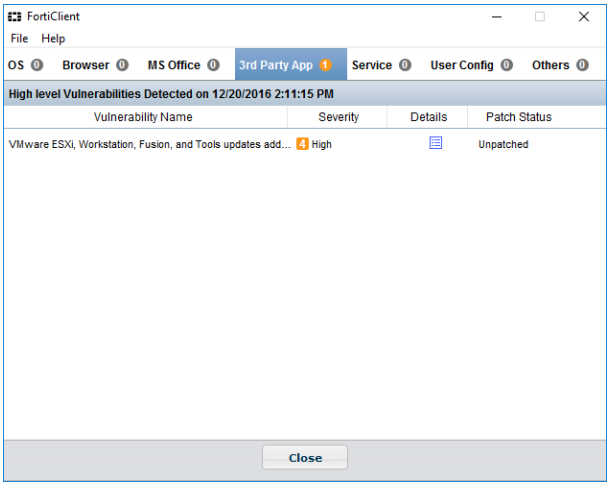
2. Download the latest software patch for each software from the Internet, and install it on the endpoint.
3. After you install the software for all remaining vulnerabilities, go to the *Vulnerability Scan* tab, and click the *Scan Now* button to instruct FortiClient to confirm that the vulnerabilities are fixed.

   If the manual fixes were successful, the *Vulnerability Scan* tab displays *Vulnerabilities Detected: None* after the scan completes.

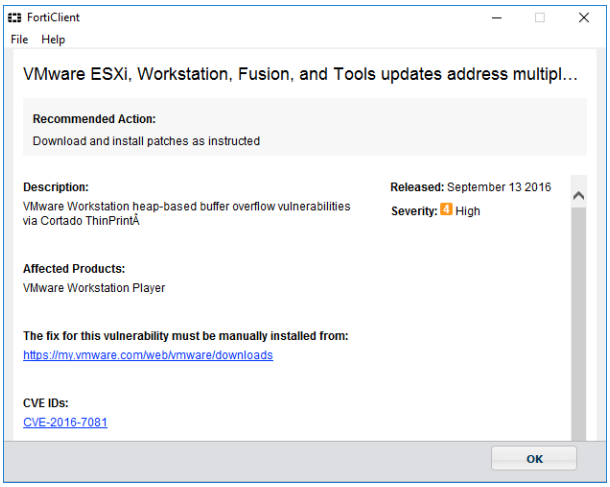
Viewing details about vulnerabilities

To view details about vulnerabilities:

1. On the *Vulnerability Scan* tab, any software with detected vulnerabilities that requires you to manually download and install software patches is displayed in the *Vulnerabilities Detected* area.
2. You can view more details by clicking the *Vulnerabilities Detected <number>* link or the category for detected vulnerabilities, such as *Critical*, *High*, *Medium*, or *Low*.
3. Click the *Details* icon.



If the detected vulnerability requires you to manually download and install a fix, it is communicated in the *Recommended Action* section. In addition, the following information is displayed: *The fix for the vulnerability must be manually installed from: <link>*.



4. Click *OK* to close the window.

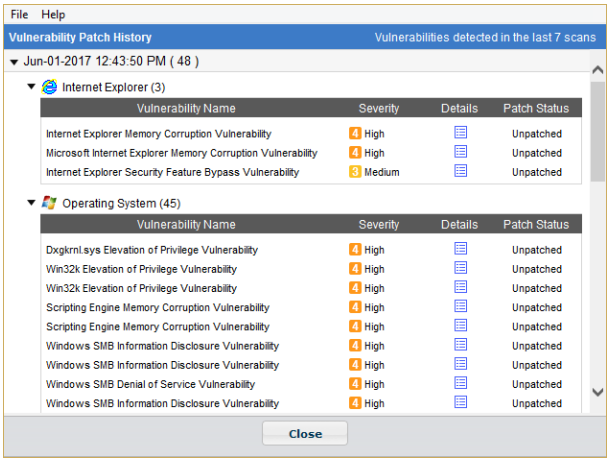
Viewing vulnerability scan history

You can view the history of last seven vulnerability scans and patches. You can view the history to see what software was identified as vulnerable and whether patches for the vulnerabilities were installed.

To view vulnerability patch history:

1. In the FortiClient console, click the *Vulnerability Scan* tab.
2. Click the *Scan History* link.

   The vulnerability patch history displays by date. Click each date and software name to expand it and view details or contract it and hide details.



3. Click *Close* to return to the *Vulnerability Scan* tab.

Settings

This section describes the options on the *File* > *Settings* page.

What options you can change on the *Settings* page depends on whether FortiClient is in standalone or managed mode. In managed mode, FortiGate or EMS may lock settings.

System

You can back up or restore a FortiClient configuration.

Backing up or restoring full configuration files

You can back up the FortiClient configuration to an XML file, and restore the FortiClient configuration from an XML file.

To backup or restore the full configuration file:

1. Go to *File* > *Settings*.
2. Expand the *System* section, then select *Backup* or *Restore* as needed.
   When performing a backup, you can select the file destination, password requirements, and add comments as needed.

Logging

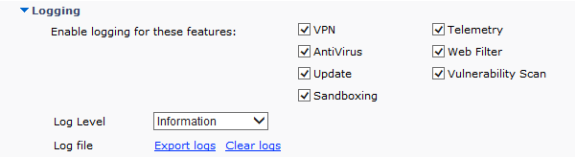
This setting can only be configured when FortiClient is in standalone mode.

Enabling logging for features

You can enable logging for modules available in FortiClient Console. Logging options are hidden for modules not available in FortiClient Console.

To enable logging for features:

1. Go to *File* > *Settings*.
2. Expand the *Logging* section.



3. Select the features for which you want to add entries to the log file:

VPN	Select *VPN* to enable logging for this feature.
Application Firewall	Select *Application Firewall* to enable logging for this feature.
AntiVirus	Select *AntiVirus* to enable logging for this feature.
Update	Select *Update* to enable logging for FortiClient software updates.
Sandboxing	Select *Sandboxing* to enable logging for this feature.
Telemetry	Select *Telemetry* to enable logging for this feature.
Web Security/Web Filter	Select *Web Security* or *Web Filter* to enable logging for this feature.
Vulnerability Scan	Select Vulnerability Scan to enable logging for this feature.

4. Select a logging level, and click *OK*.

Emergency	The system becomes unstable.
Alert	Immediate action is required.
Critical	Functionality is affected.
Error	An error condition exists and functionality could be affected.
Warning	Functionality could be affected.
Notice	Information about normal events.
Information	General information about system operations.
Debug	Debug FortiClient.

It is recommended to use the debug logging level only when needed. Do not leave the debug logging level permanently enabled in a production environment to avoid unnecessarily consuming disk space.

Sending logs to FortiAnalyzer or FortiManager

The following products are required for an administrator to configure FortiClient in managed mode to send logs to FortiAnalyzer or FortiManager:

- FortiClient
- FortiGate or EMS
- FortiAnalyzer or FortiManager

When FortiClient connects Telemetry to FortiGate or EMS, the endpoint can upload logs to FortiAnalyzer or FortiManager units on port 514 TCP.

Where you locate FortiClient logs in FortiAnalyzer depends on where FortiClient Telemetry is connected:

- When FortiClient connects Telemetry to EMS, the FortiClient logs are displayed in the FortiClient ADOM in FortiAnalyzer. In this scenario FortiGate is not used.
- When FortiClient connects Telemetry to FortiGate, the FortiClient logs are displayed in the FortiGate ADOM. Even if EMS is used with FortiGate to manage FortiClient endpoints, the FortiClient logs still display in the FortiGate ADOM.

FortiClient Telemetry must connect to FortiGate or EMS for FortiClient to upload logs to FortiAnalyzer or FortiManager.

Exporting the log file

You can export the log file (`.log`) from FortiClient.

To export log files:

1. Go to *File* > *Settings*.
2. Expand the *Logging* section, and click the *Export logs* link.
   The *Save As* dialog box displays.
3. Select a location for the log file, type a name for the log file, and click *Save*.

Clearing entries in the log file

To clear entries in the log file:

1. Go to *File* > *Settings*.
2. Expand the *Logging* section, and click the *Clear logs* link.
   A confirmation dialog box displays.
3. Click *Yes* to confirm.
   The contents of the log file are deleted, and a confirmation dialog box displays.
4. Click *OK*.

VPN options

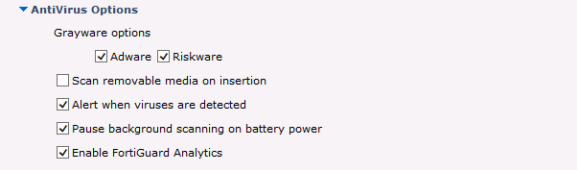
To configure VPN options:

1. Go to *File* > *Settings* from the toolbar, and expand the *VPN* section.
2. Select *Enable VPN before logon* to enable VPN before log on.
3. Click *OK*.

Antivirus options

To configure antivirus options:

1. Go to *File* > *Settings*, and expand the *Antivirus Options* section.



2. Configure the following settings, and click *OK*:

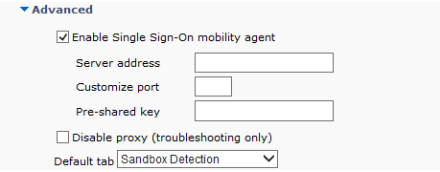
Grayware options	Grayware is an umbrella term applied to a wide range of malicious applications such as spyware, adware, and key loggers that are often secretly installed on a user's computer to track and/or report certain information back to an external source without the user's permission or knowledge.
Adware	Select to enable adware detection and quarantine during the antivirus scan.
Riskware	Select to enable riskware detection and quarantine during the antivirus scan.
Scan removable media on insertion	Select to scan removable media when it is inserted.
Alert when viruses are detected	Select to have FortiClient provide a notification alert when a threat is detected on your personal computer. When *Alert when viruses are detected* under *AntiVirus Options* is not selected, you will not receive the virus alert dialog box when attempting to download a virus in a web browser.
Pause background scanning on battery power	Select to pause background scanning when your computer is operating on battery power.
Enable FortiGuard Analytics	Select to automatically send suspicious files to the FortiGuard Network for analysis.

Advanced options

These settings can be configured only when FortiClient is in standalone mode. When FortiClient Telemetry is connected to FortiGate or EMS, these settings are set by the XML configuration (if configured).

To configure advanced options:

1. Go to *File* > *Settings*, and expand the *Advanced* section.



2. Configure the following settings, and click *OK*:

Enable Single Sign-On mobility agent	Select to enable single sign-on mobility agent for FortiAuthenticator. To use this feature you need to apply a FortiClient SSO mobility agent license to your FortiAuthenticator device.
Server address	Enter the FortiAuthenticator IP address.
Customize port	Enter the port number. The default port is 8001.
Pre-shared Key	Enter the preshared key. The preshared key should match the key configured on your FortiAuthenticator device.
Disable proxy (troubleshooting only)	Select to disable proxy when troubleshooting FortiClient.
Default tab	Select the default tab to be displayed when opening FortiClient.

Single Sign-On mobility agent

The FortiClient Single Sign-On (SSO) mobility agent is a client that updates FortiAuthenticator with user logon and network information.

FortiClient/FortiAuthenticator protocol

FortiAuthenticator listens on a configurable TCP port. FortiClient connects to FortiAuthenticator using TLS/SSL with two-way certificate authentication. FortiClient sends a logon packet to FortiAuthenticator, which replies with an acknowledgment packet.

FortiClient/FortiAuthenticator communication requires the following:

- The IP address should be unique in the entire network.
- FortiAuthenticator should be accessible from clients in all locations.
- All FortiGates should be able to access FortiAuthenticator.

FortiClient Single Sign-On mobility agent requires FortiAuthenticator running 2.0.0 or later, or 3.0.0 or later. Enter the FortiAuthenticator (server) IP address, port number, and the preshared key configured on FortiAuthenticator.

To enable Single Sign-On mobility agent on FortiClient:

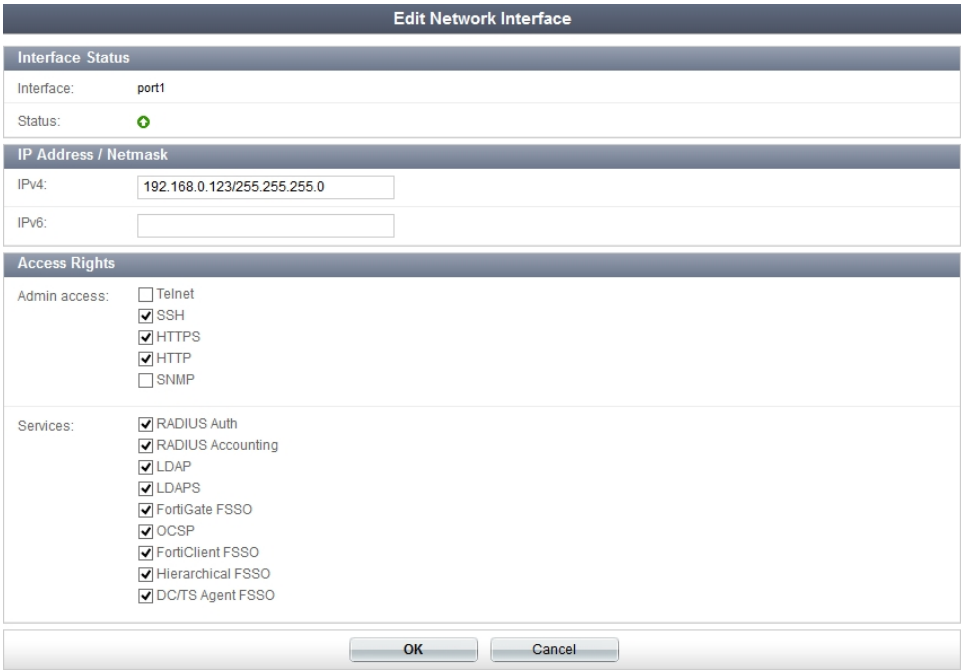
1. In FortiClient Console, go to *File* > *Settings*.
2. Expand the *Advanced* section and select *Enable Single Sign-On mobility agent*.
3. Type the FortiAuthenticator server address and the preshared key.
4. Click *OK*.

To enable FortiClient SSO mobility agent service on the FortiAuthenticator:

1. In FortiAuthenticator, select *Fortinet SSO Methods* > *SSO* > *General*. The *Edit SSO Configuration* page opens.
2. Select *Enable FortiClient SSO Mobility Agent Service* and enter a TCP port value for the listening port.
3. Select *Enable authentication* and enter a secret key or password.
4. Select *OK* to save the setting.

To enable FortiClient FSSO services on the interface:

1. Select *System* > *Network* > *Interfaces*. Select the interface and select *Edit* from the toolbar. The *Edit Network Interface* window opens.



2. Select the checkbox to enable *FortiClient FSSO*.
3. Click *OK* to save the setting.

To enable the FortiClient SSO mobility agent service on FortiAuthenticator, you must first apply the applicable FortiClient license for FortiAuthenticator. See the *FortiAuthenticator Administration Guide* in the Fortinet Document Library.

For information on purchasing a FortiClient license for FortiAuthenticator, contact your authorized Fortinet reseller.

Configuration lock

This setting can only be configured when FortiClient is in standalone mode.

You can prevent unauthorized changes to the FortiClient configuration by locking the configuration. When the configuration is locked, configuration changes are restricted and FortiClient cannot be shut down or uninstalled.

When the configuration is locked, you can perform the following actions on the *Settings* page:

- Back up the FortiClient configuration
- Export FortiClient logs

If you want to change the configuration or shut down FortiClient, you must unlock the configuration first.

To lock the configuration:

1. Go to *File* > *Settings*.
2. Click the unlocked icon in the bottom left corner.
3. In the *Password* box, type a password.
   Ensure you remember the password. You will need to use it to unlock the configuration.
4. In the *Confirm* box, retype the password.
5. Click *OK*.

To unlock the configuration:

1. Go to *File* > *Settings*.
2. Click the locked icon in the bottom left corner.
3. In the *Password* box, type the password used to lock the configuration.
4. Click *OK*.

FortiTray

When FortiClient is running on your system, you can select the FortiTray icon in the Windows system tray to perform various actions. The FortiTray icon is available in the system tray even when FortiClient Console is closed.

- Default menu options:
  - Open FortiClient Console
  - Shut down FortiClient

- Dynamic menu options, depending on configuration:
  - Connect to a configured IPsec VPN or SSL VPN connection
  - Display the antivirus scan window (if a scheduled scan is currently running)
  - Display the Vulnerability scan window (if a vulnerability scan is running)

If you hover the mouse cursor over the FortiTray icon, you will receive various notifications including the version, antivirus signature, and antivirus engine.

When the configuration is locked, the option to shut down FortiClient from FortiTray is grayed out.

Establishing VPN connections from FortiTray

To establish a VPN connection from FortiTray:

1. Select the Windows System Tray.
2. Right-click the *FortiTray* icon, and select a VPN connection configuration.
3. Type your username and password in the authentication window, and click *OK* to connect.

Diagnostic Tool

You can access the FortiClient Diagnostic Tool from FortiClient Console. Go to *Help* > *About*.

On FortiClient (Windows), you can also access the Diagnostic Tool from the *Start* menu.

You can use the FortiClient Diagnostic Tool to generate a debug report, then provide the debug report to the FortiClient team to help with troubleshooting. For example, if you are working with customer support on a problem, you can generate a debug report and email the report to customer support to help with troubleshooting.

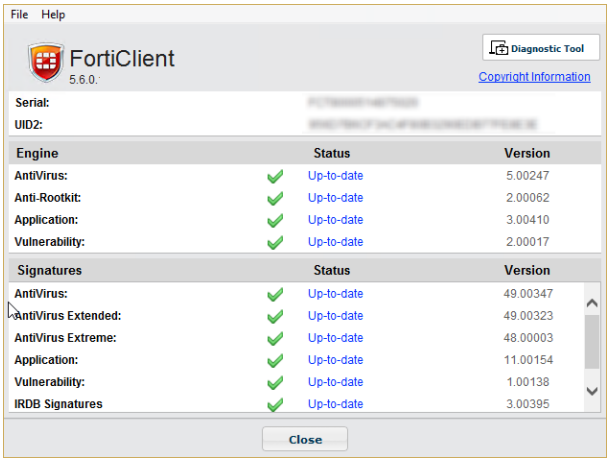
The FortiClient Diagnostic Tool does not record sensitive information. It contains information about the endpoint such as:

- Windows operating system version
- Windows software updates
- Names and versions of installed software
- Names and versions of installed drivers
- FortiClient configuration
- FortiClient logs

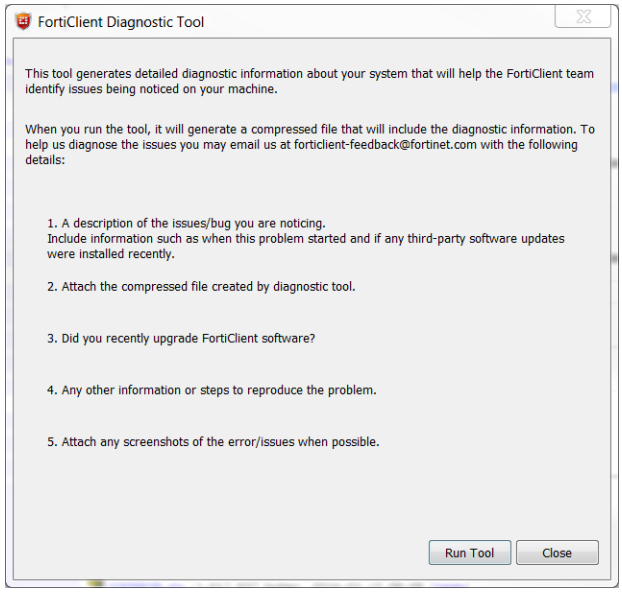
Before sending the package created by FortiClient Diagnostic Tool, you can open and read the package.

To generate debug reports:

1. Go to *Help* > *About*.

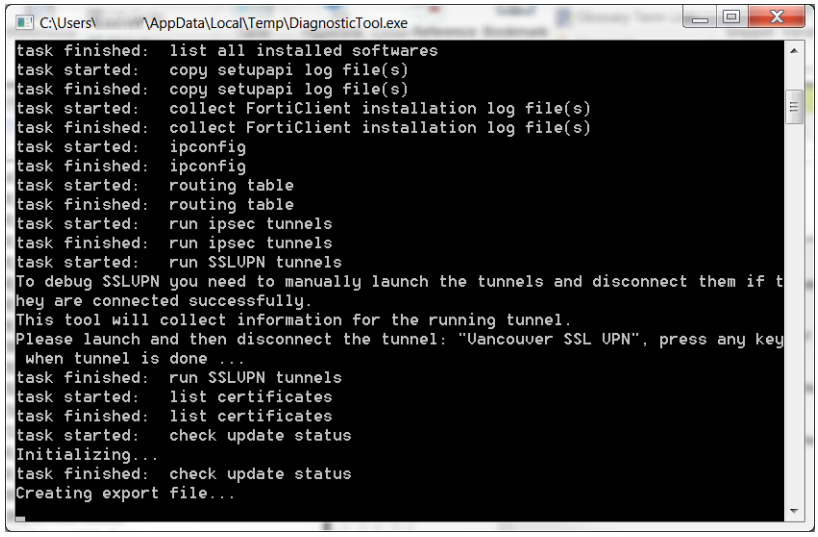


2. Click the *Diagnostic Tool* button in the top right corner. The FortiClient Diagnostic Tool dialog box displays.



3. Click *Run Tool*.

   A window displays the provides status information.



4. (Optional) When prompted, launch and disconnect the VPN tunnels for which you want to collect information.

   A *Diagnostic_Result* file is created and displays in a folder on the endpoint. The default folder location is *C:\Users <user name>\AppData\Local\Temp*.

5. Click *Close*.

Appendix A - FortiClient API

You can operate FortiClient VPNs using the COM-based FortiClient API. The API can be used with IPsec VPN only. SSL VPN is currently not supported.

Overview

The FortiClient COM library provides functionality to:

- Retrieve a list of the VPN tunnels configured in the FortiClient application.
- Start and stop any of the configured VPN tunnels.
- Send XAuth credentials.
- Retrieve status information:
  - configured tunnel list
  - active tunnel name
  - connected or not
  - idle or not
  - remaining key life
- Respond to FortiClient-related events:
  - VPN connect
  - VPN disconnect
  - VPN is idle
  - XAuth authentication requested

For more information, see the vpn_com_examples ZIP file located in the VPN Automation file folder in the FortiClientTools file.

API reference

The following tables provide API reference values.

`Disconnect(bstrTunnelName As String)`	Close the named VPN tunnel.
`GetPolicy pbAV As Boolean, pbAS As Boolean, pbFW As Boolean, pbWF As Boolean)`	Command is deprecated in FortiClient v5.0.
`GetRemainingKeyLife(bstrTunnelName As String, pSecs As Long, pKBytes As Long)`	Retrieve the remaining key life for the named connection. Whether keylife time (pSecs) or data (pKBytes) are significant depends on the detailed settings in the FortiClient application.

`MakeSystemPolicyCompliant()`	Command is deprecated in FortiClient v5.0.
`SendXAuthResponse (tunnelName As String, userName As String, password As String, savePassword As Boolean)`	Send XAuth credentials for the named connection: • User name, Password • True if password should be saved.
`SetPolicy (bAV As Boolean, bAS As Boolean, bFW As Boolean, bWF As Boolean)`	Command is deprecated in FortiClient v5.0.
`GetTunnelList()`	Retrieve the list of all connections configured in the FortiClient application.
`IsConnected (bstrTunnelName As String) As Boolean`	Return True if the named connection is up.
`IsIdle (bstrTunnelName As String) As Boolean`	Return True if the named connection is idle.
`OnDisconnect(bstrTunnelName As String)`	Connection disconnected.
`OnIdle(bstrTunnelName As String)`	Connection idle.
`OnOutOfCompliance(bAV As Boolean, bAS As Boolean, bFW As Boolean, bWF As Boolean)`	Command is deprecated in FortiClient v5.0.
`OnXAuthRequest(bstrTunnelName As String)`	The VPN peer on the named connection requests XAuth authentication.

Appendix B - FortiClient Log Messages

For a list of FortiClient log messages, see the FortiClient 5.6.4 Online Help at http://docs.fortinet.com/forticlient/admin-guides. The table of log messages is too wide to fit into the page size of the *FortiClient 5.6.4 Administration Guide*.

Appendix C - Vulnerability Patches

FortiClient checks many applications for vulnerabilities. FortiClient can automatically patch vulnerabilities from some applications, but not all applications. For some applications, the user must manually patch vulnerabilities.

For the latest list of supported software, see the FortiGuard Center (FortiGuard.com) .

FortiClient (Windows)

Automatic vulnerability patching

FortiClient (Windows) automatically patches vulnerabilities for the following software:

- 7-Zip
- Microsoft Bulletin
- Apple iTunes
- Mozilla Firefox
- Mozilla Firefox ESR
- Foxit Reader
- Java JRE
- Wireshark
- Mozilla Thunderbird
- Adobe Air
- Adobe Acrobat
- Adobe Acrobat DC
- Adobe Reader
- Adobe Acrobat Reader DC
- Adobe Flash Player Active X plug-in for Internet Explorer
- Adobe Flash Player NPAPI plug-in for Firefox
- PostgreSQL (version 9.1 or later)
- VideoLAN VLC Media Player
- VMware Player
- VMware Workstation Player

Manual vulnerability patching

FortiClient (Windows) automatically checks the following software for vulnerabilities, but cannot automatically patch vulnerabilities. The user must manually locate, download, and install updates to the following software to patch vulnerabilities:

- Adobe AIR SDK
- Adobe Acrobat X

- Adobe Acrobat Reader X
- Adobe Shockwave Player
- Apple QuickTime
- Apple Safari
- Jave JDK
- Google Chrome
- Google Picasa
- Oracle MySQL server
- PHP
- PostgreSQL (earlier than version 9.1)

FortiClient (OS X)

Automatic vulnerability patching

FortiClient (OS X) automatically patches vulnerabilities for the following software:

- Adobe Acrobat
- Adobe Acrobat DC
- Adobe Acrobat Reader DC
- Adobe Flash Player NPAPI plug-in
- Apple products
- Mozilla Firefox
- Mozilla Firefox ESR
- Google Chrome
- Java JRE
- SeaMonkey
- Mozilla Thunderbird
- Mozilla Thunderbird ESR
- VideoLAN VLC Media Player
- VMware Fusion
- Wireshark
- PostgreSQL
- Foxit Reader

Manual vulnerability patching

FortiClient (OS X) automatically checks the following software for vulnerabilities, but cannot automatically patch vulnerabilities. The user must manually locate, download, and install updates to the following software to patch vulnerabilities:

- Adobe AIR SDK
- Java JDK
- MySQL Server

- Adobe Reader
- Moodle

Appendix D - FortiClient Processes

This section identifies the processes used by FortiClient (Windows) and FortiClient (OS X).

FortiClient (Windows) processes

The following table identifies the processes in Task Manager used by FortiClient (Windows):

Process Name	Process Purpose
FortiClient Application Database Service	Network Access Control (NAC) and Antivirus
FortiClient Console	FortiClient GUI
FortiClient IPsec VPN Service	Remote Access for IPsec VPN
FortiClient Firewall Service	Application Firewall
FortiClient Logging Daemon	Logging
FortiClient Diagnostic Tool	Diagnostic Tool
FortiClient Network Access Control	FortiClient Telemetry
FortiClient Proxy Service	Antivirus and Web Filter
FortiClient Realtime AntiVirus Protection	Antivirus
FortiClient Sandbox Agent	Sandbox Detection
FortiClient Scan Server	Antivirus to offload Antivirus scanning to a separate process
FortiClient Scheduler	Windows ensures that FortiClient services are running when needed
FortiClient SSLVPN daemon	Remote Access for SSL VPN
FortiClient System Helper	FortiClient ensures that 32-bit processes can access 64-bit resources
FortiClient System Tray Controller	FortiTray
FortiClient User Avatar Agent	FortiClient Console and FortiClient Telemetry use to obtain avatar images for users
FortiClient Virus Feedback Service	Antivirus and FortiClient Console use to submit samples to FortiGuard
FortiClient Vulnerability Scan Daemon and Engine	FortiClient Vulnerability Scan engine
FortiClient Web Filter Service	Used by Web Filter

FortiClient (OS X) processes

FortiClient (OS X) uses the following processes:

- The process for FortiClient main GUI is located at `/Application/FortiClient.app/Contents/MacOS/FortiClient`
- The process for FortiTray controller is located at `/Application/FortiClient.app/Contents/Resources/runtime.helper/FortiClientAgent.app/MacOS/FortiClientAgent`
- The process for FortiClient upgrade GUI is located at `/Application/FortiClient.app/Contents/Resources/runtime.helper/FortiClientUpdate.app/Contents/MacOS/FortiClientUpdate`

The following table identifies the processes in the following location used by FortiClient (OS X):

`/Library/Application Support/Fortinet/FortiClient/bin`:

Process Name	Process Purpose
fctservctl	FortiClient Service Controller
epctrl	FortiClient endpoint control daemon
ftgdagent	Web Filter
fmon	AntiVirus scan main program
scanunit	AntiVirus scan scanner
vulscan	Vulnerability scan
fctappfw	Firewall Service
fssoavgent_launchagent	FortiClient single sign on agent
fssoavgent_launchdaemon	FortiClient single sign on daemon
fctctld	VPN controller
sslvpnd	SSL VPN Daemon
racoon	IPsec VPN Service
racoonctl	IPsec VPN Controller
fctupdate	FortiClient update tool
fctupgrade	FortiClient upgrade tool
fcconfig	FortiClient Configurator tool